

NAVY SOCIAL MEDIA HANDBOOK

FOR ADMINISTRATORS & PAOs

2023



Updated:
February 10, 2023

For social media queries
please email:
NavySM@us.navy.mil

Page Intentionally Left Blank



ASSISTANT TO THE SECRETARY OF DEFENSE

1400 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1400

DEC 20 2021

Public Affairs

MEMORANDUM FOR MILITARY SERVICE CHIEFS OF PUBLIC AFFAIRS NATIONAL GUARD CHIEF OF PUBLIC AFFAIRS

SUBJECT: Core Operational Principles on the Use of Official Social Media Accounts within the Department of Defense

While the information and technological environment continue to evolve, our professional and ethical conduct must remain steadfastly aligned to the highest core principles of our service to the Nation.


The Department of Defense's (DoD) reputation for transparency rests in large part on the foundation of the Department's Principles of Information contained in DoD Directive 5122.05, "Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))," and the Department's adherence to these standards. DoD's use of official social media plays an important role in ensuring a free flow of information to the public consistent with these principles. In accordance with DoD Directive 5122.05 and DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," I am sharing these core principles to guide departmental use of official social media accounts and to set expectations of proper conduct for all official account holders.

The core operational social media principles are described below.

1. **Governance.** Public Affairs oversees and manages official DoD social media accounts. This ensures proper alignment with communication and information plans across all media and social media platforms.
2. **Professionalism.** All official social media content reflects upon the Department. Public Affairs Officers and social media administrators must exercise the same high standard of professional and ethical behavior on these accounts as with any other communication function or capability. Official social media accounts must not be used to promote or endorse non-Federal entities or personal financial interests.
3. **Propriety.** Information authorized and publicly released by DoD constitutes official DoD information; therefore, accuracy, appropriateness, timeliness, and proper tone are imperative.
4. **Acumen.** Official social media account administrators should have current knowledge of social media tactics, best practices, and trends, coupled with an understanding of public affairs objectives (e.g., DoD Communication Playbook) to act quickly and remain effective by properly employing social media to meet Departmental objectives in an appropriate manner.

5. **Establishment Appetite.** Establishing new official social media accounts should be carefully considered against existing accounts and platforms. More for the sake of more is not necessarily better.
6. **Transparency.** Content, including replies, will not be deleted from official accounts unless there is a factual or typographical error; violation of a law, policy, term of service, or user agreement; or a security concern. Removal of content will be publicly acknowledged and communicated to audiences to provide context and clarity of the action.
7. **Retention of Content:** DoD social media posts are agency records pursuant to the Federal Records Act (44 U.S.C Chapters 31 and 33). Public Affairs Officers and social media administrators are responsible for retaining information posted to their respective social media sites in accordance with the guidance provided by their DoD component records managers.

As leaders, public affairs practitioners, professional communicators, and public servants, we will continue to advance and improve the quality of information that we share with all DoD audiences, the news media, and the American public. These principles, coupled with a pending DoD instruction on social media usage, are necessary to sustain the trust and credibility of our message on a global information stage.



John F. Kirby

Cc:

Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
Chiefs of the Military Services
Chief of the National Guard Bureau
Commanders of the Combatant Commands
General Counsel of the Department of Defense
Chief Information Officer of the Department of Defense
Assistant Secretary of Defense for Special Operations and Low Intensity Conflict

TABLE OF CONTENTS

2	Overview	56	Appendix A: Acceptable Use Policy
3	Before Starting a Presence: Considerations	58	Appendix B: Required Disclaimer
7	Audiences	59	Appendix C: References
11	Platform Demographics	60	Appendix D: User Persona Templates
16	Planning Considerations	61	Appendix E: Key Channels Template
17	The Age of the Influencer	62	Appendix F: Channel Optimization Template
18	Registering Your Social Media Presence	63	Appendix G: Format Specs Per Platform
20	Platform Selection	67	Appendix H: Blank Planning Calendar
21	Audiences	68	Appendix I: Calendar Dates
23	Setting Goals & Objectives	70	Appendix J: Naval History Dates of Interest
24	Key Channels	81	Appendix K: Political Activity
26	Content Planning	90	Appendix L: DoD Instruction 5400.17 Official Use of Social Media For Public Affairs Purposes
28	Content Mediums		
29	Content Creation & Distribution		
30	Best Practices Per Platform		
32	Crisis Communication		
33	Areas of Potential Risk		
34	Individual Responsibility		
35	The UCMJ & Navy Regulations		
38	Bots		
39	Guidance		
42	DoD Personnel and Political Activity: The Hatch Act		
43	Resources		
45	How To's		
50	On the Horizon		
52	Navy Social Media Fo'c'sle		
53	Glossary		



DEEP DIVE: SOCIAL MEDIA HANDBOOK FOR ADMINS

Communicating in an ever-changing environment requires that our communication be agile enough to remain effective and lands in the digital space intended, while it resonates and informs the wider audiences we wish to reach. Social media is therefore a necessity vice a nice-to-have. Operating efficiently in the social media space means much more than “I have a Facebook account.”

OVERVIEW

Social media, when used effectively and responsibly, presents an opportunity to share the U.S. Navy story in an authentic, transparent, and rapid way by building relationships with a much broader audience in the online community.

Because social media is the fastest way to disseminate timely information, planning for social media should be an integral part of your communication strategy from the beginning of the planning process. When approached as an afterthought, it cannot reach its full potential.

Facilitating the free flow of information while preserving security, respecting privacy, and maintaining proper conduct online are critical considerations for all social media users. It is everyone's responsibility to ensure information disclosed or shared online does not violate applicable policy or law, jeopardize operations security (OPSEC), adheres to strong identity management (IdM) best practices, and protects the safety and privacy of U.S. Government personnel and their families.

Of course, as with every communication tool, appropriate precautions, guidelines, and best practices must be developed prior to execution. The U.S. Navy Social Media Handbook covers platforms, describes audiences, tackles content planning, and addresses how to develop meaningful objectives to accomplish communication goals.

By staying aware of the latest trends and tools in the digital space, social media can elevate the Navy story and reach new audiences never thought possible.

Let's dive in!

Produced by
The Navy Office of Information (CHINFO)



Mention of a commercial product or service in this document does not constitute official endorsement by the U.S. Navy, the Department of Defense or the federal government.

BEFORE STARTING A PRESENCE: CONSIDERATIONS

Should I Or My Command Have a Social Media Presence?

There are multiple avenues on which to publish content. These spaces are referred to as social media platforms, networks, or channels. Some are widely familiar such as Facebook, and others are continuously emerging and gaining traction week to week and month to month. Not every platform is an appropriate fit for communicating your messages and/or achieving your communication objectives.

Determining which platforms to utilize largely depends on two factors:

1. Which audiences are you attempting to reach; and on which platforms do they engage?
2. Can you meet the appropriate posting frequency, content demands, and engagement responsiveness the audiences of these platforms demand?

To answer the above and determine where you should be, have your staff research each platform to determine which make sense for your available content and desired messaging. Evaluate where your efforts will have the most impact.

*** Note: Not only is it unnecessary, but it is counterproductive to maintain a presence on every social media platform. (See Platform Demographics for basic platform information and audience breakdown.)

Quality > Quantity: Select **quality** of content/messaging/engagement with your desired audience, over **quantity** of social media accounts.



What do you want to accomplish? What are your communication objectives? How do they move your command closer to achieving its mission? Is the level of transparency required in social media appropriate for your command and its mission? Do you have the content and personnel to routinely engage with the desired audiences?

Do You Have the Bandwidth?

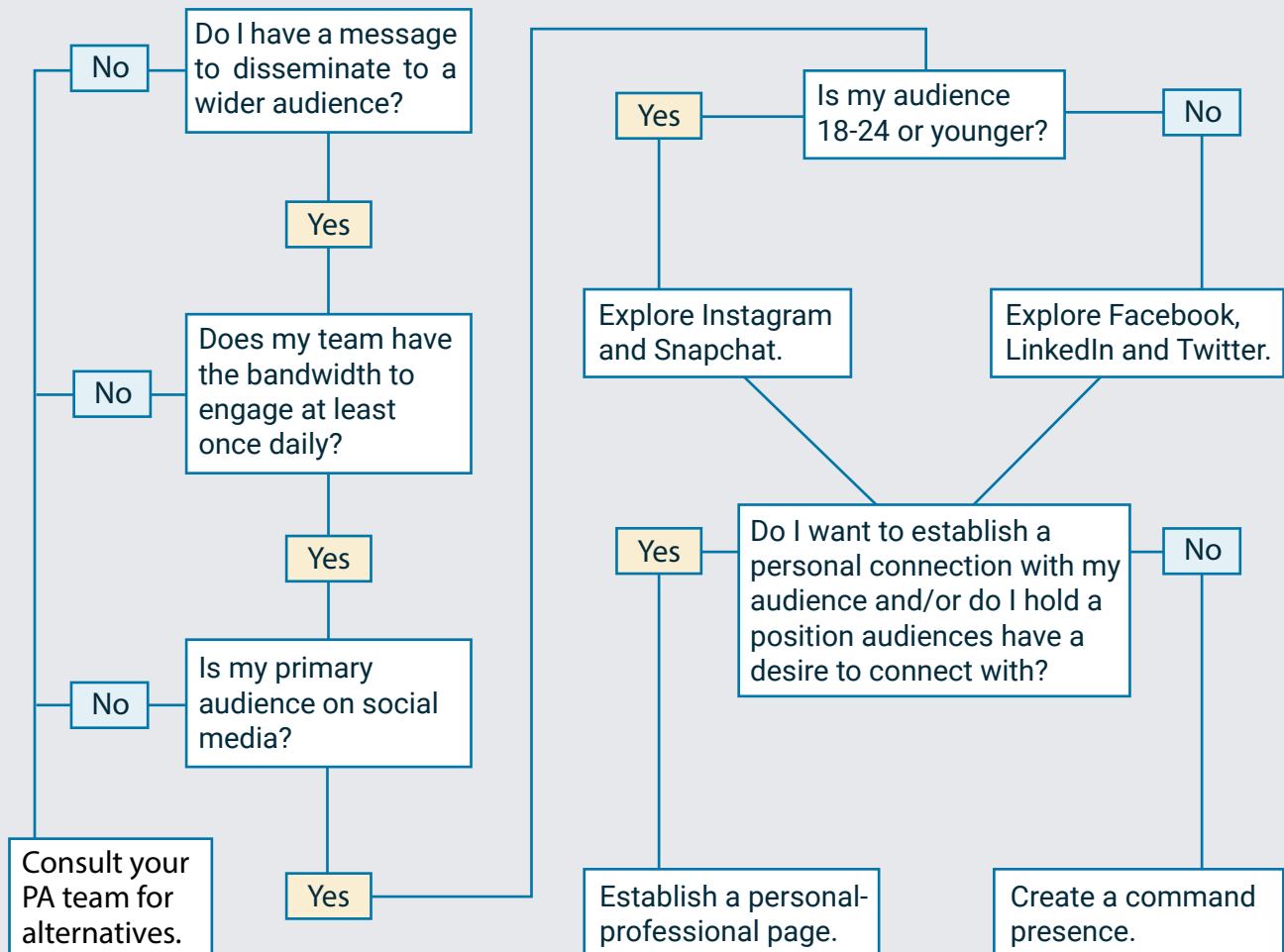
A platform is only as good and as effective as the content posted to it. It is important to have reliable access to monitor and engage audiences as necessary. Social media is not a fire-and-forget system!

When your content is infrequent, but no less important, one option is having your staff push content to more senior organizations to share — your higher command HQ or the Navy Flagship accounts managed by the Navy Office of Information (CHINFO), for example.



If you do have the staffing to publish content regularly to a platform, the next question is whether you need a personal professional page or a command presence or both? And if both, what the purpose of each will be. There should be clear communication objectives for each; the personal/professional page is more first-person with a behind the scenes tone in order to better connect with the audience whereas a command presence is more formal and not attached to a particular individual or principal.

Decision Tree For Leaders



Official Organizational Account

An official command presence is a page listed by the name of your command and that pushes out content to tell the story of that particular command and mission writ large. These pages speak officially on behalf of that command to include news, press releases, Sailor life, and other pertinent subject matter; infusing command messages throughout.

Personal Pages

A personal page, conversely, is a non-official page not tied in any way to the Navy or the uniform. This is your own presence for your close friends and family. Personal pages should NOT be used to announce official DoD information.

Personal-Professional Pages

A personal-professional page is an official page where you represent yourself as an individual, but also represent your office/position in a professional capacity. There are two types of personal-professional pages.

1. Official Institutional Accounts. These are accounts that are denominated only with an official position title, for example @SECDEF or @DepSecDef.

2. Official Individual Accounts. These include a personal name or identifier, for example: @DASDSmith.

The former is preferred over the latter due to the custom name associated with the page that will have to, by instruction, be passed to the successor of that position or taken down altogether.

Leaders should be prepared for Sailors, families, the general public, etc. to reach out via direct message for emergencies, grievances or personal issues. Please consult your PA teams as to the best solution given your time constraints. Solutions may include: placing a central POC in the about section (PA Office, Public Inquiries line, etc.), disabling DMs, or referring them to the appropriate POC.

If you're considering a personal-professional page, one thing that must be kept in mind is the number of impersonation pages that will likely pop up. Though most are not cause for alarm, they can cause some angst amongst PA teams and security personnel. In order to help thwart these efforts and enable audiences to distinguish between real and fake presences, have your PA teams work to obtain page verification.



Professional Page

Source: Twitter@SecDef



Personal Page

! This example does Not reflect a real Twitter page. For demonstration purposes only.





Verification Example

Source: Twitter@USNavy

What Is Page Verification?

Page verification is essentially a blue badge with a checkmark associated with an account that lets people know the page is authentic and verified by the platform. These blue badges appear on Facebook, Twitter and Instagram and convey that a given page is a credible source for information and/or a legitimate representation of the individual or organization it claims to be. Twitter verification is now in flux given their change in leadership, but the badges still distinguish accounts as valid and are still recommended. LinkedIn has worked very hard to ensure their registration process catches any imposters up front and therefore badges are not used on that platform as of yet.

Why Get Verified?

As with all good things, bad actors can use social media for nefarious purposes. While having a presence has definite communication benefits (and is encouraged), it also carries the risk that actors will impersonate you and/or your command. More and more scams are being seen where photos are used to create imposter profiles which solicit money, information, or seek to discredit or embarrass the individual and/or the Navy. For more on Twitter as it continues to shift, please stay plugged in to OI-2 Fleet Content meetings.

“ One way to ensure your audiences know it’s you, is to get verified. Think of it as a “firewall” for your account, as this helps audiences distinguish between official/real pages and impersonator pages at a glance. ”

How To Get Verified

To get your page(s) verified, have your PA team reach out to CHINFO OI-2 at **NavySM@us.navy.mil**. They will need to have your About/Bio sections fully filled out with current working links to bio pages on **Navy.mil** (for personal professional pages) or command page on **Navy.mil** (for organization pages), provide email addresses of admins to the page(s), and the URLs for the pages.

*** Please be patient as this process CAN and DOES take time, because platforms must review each presence for certain criteria. This could take from two weeks to two months depending on the platform and current events.



Personal accounts should not be used to announce official DoD information.



Reporting Fake Pages

If you or your team notice fake/impersonator pages made in your likeness or under your command name/logo, have your team do the following:

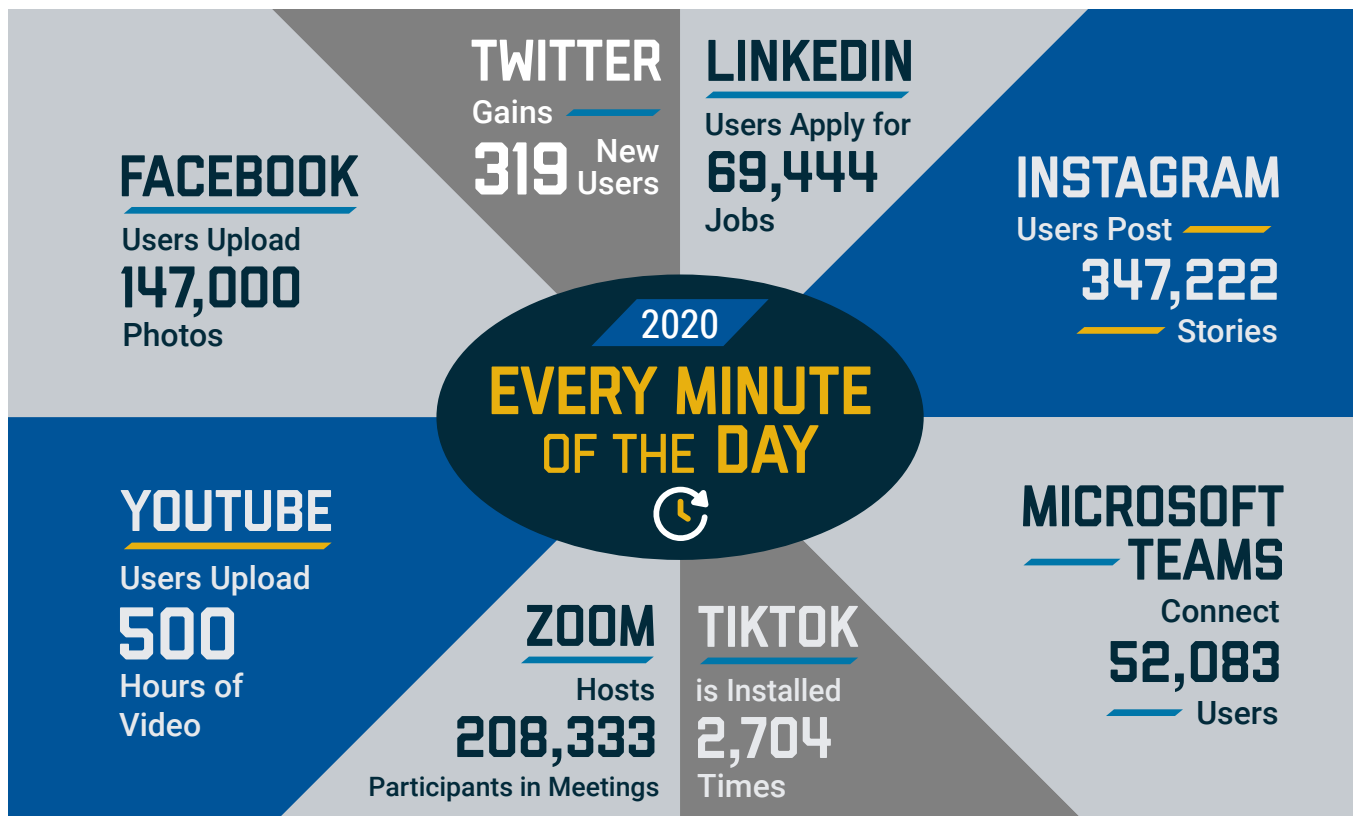
1. Report it within the platform (for Twitter, this will yield a case number).
2. Send links to the impersonator pages as well as a link to your REAL page(s) to CHINFO, OI-2 at **NavySM@us.navy.mil** for action.
3. If this becomes a trend, please also report to NCIS.

AUDIENCES

One of the most important components of maintaining a successful and effective presence on social media is clearly defining your target audience, understanding their expectations, curiosities, and “meeting them where they’re at.” Tailor the language in your messages in such a way that your intended audience will be receptive and engaging.

Audience-First Approach

When there were a limited number of news sources, we could package news, pitch it, get it published; and expect it to be consumed. Today, with a 24-hour news cycle, and so many different entities competing for the audiences’ attention, we must put the audience at the forefront of our planning – where do they consume information? In what mediums do they most consume/absorb information? How can I obtain and maintain their attention? This is difficult and requires continuous evaluation and innovation; and perhaps an element of risk.



Source: <https://www.visualcapitalist.com/every-minute-internet-2020/>



Who Do We Want To Talk To And Where Can We Find Them?

- **Journalists:** Journalists and celebrities often maintain a significant presence on Twitter, a fast-paced, news source and amplification platform. Though they are certainly found on other platforms. Twitter is the space in which we primarily talk to and engage with them and is where they are going for their news as well. Many use Twitter to gauge what is happening before digging deeper on other or more traditional platforms.
- **Sailors and Families:** This is age dependent. Much like their civilian counterparts, 18-34 year old Sailors are likely to be found on Instagram Reels, Snapchat, and TikTok (NOT approved for use on DoD devices), while 34+ are more likely to be found on Facebook and LinkedIn. Sailors tend to hang in the background on Facebook until issues related to pay, allowances and uniform changes arise.
- **Local Community:** Same as above; however, hashtags and geotags are very effective in connecting with your local community. Hash-tagging the town, county etc. where your command resides and/or adding location tags for special events (after they take place for OPSEC reasons; UNLESS it's an outreach event where you are hoping to boost attendance) works very well in better connecting with the local community.
- **Veterans:** We find the largest percentage of our Veteran audience on Facebook, with younger Vets gravitating a bit more to Instagram.
- **Partnership Nations/Allies:** Our allies and partners tend to engage with us most on Twitter and Instagram. Tagging their pages in your posts — during joint exercises, for example — is a great way to engage.
- **Civilian Workforce:** The Civilian workforce, much like the Sailor audience, spans all channels. However, for connecting with human resources (HR), hiring, and recruiting, LinkedIn is the best place to connect and make an impact. Most commands do not have a LinkedIn presence and LinkedIn is one area where we particularly encourage submission of information and products to CHINFO for inclusion on the U.S. Navy page.
- **Industry:** LinkedIn is where we engage most with industry, though they pay attention to Twitter as well. LinkedIn allows us to position the Navy as a thought-leader in the industrial space in areas from HR to Science Technology Engineering and Math (STEM).
- **Academia:** Twitter and LinkedIn are likely the best places to reach faculty. (Although, University and college brands overall have become more actively engaged where their student audiences live — Instagram, Snapchat, etc.)
- **Congress/HASC/SASC:** Twitter is the best place to reach these audiences.
- **Potential Recruits:** We find potential recruits engaging with us most heavily on Instagram, and some on Snapchat. Potential recruits seek positive spaces on which to engage and ask questions of those who have served to get a sense of what to expect. Creative and humorous memes do particularly well with this audience.





Adversaries and Competitors Are Listening...

We **MUST** remain vigilant and be aware of these audiences as well. Their monitoring and consumption of messages should be taken into consideration when planning content on platforms. Any mission-related information you voluntarily post on social media (personal accounts included) can potentially assist the adversary's intelligence collection activities. Additionally, misinformation and disinformation attempts from adversaries using bots and/or memes **MUST** be countered with factual and consistent information.

Tone and Voice

Just as you likely speak differently with your spouse or friends than you would, say, to your parents – the way in which you communicate on each platform should vary by the audience that is there. The tone and the voice you hone on each respective platform should speak to the primary audience of that platform in a way in which they will understand it and most positively receive it. This applies to the post copy, the content itself, and the responses to comments on a given platform. There are many ways to get a point across; and though the voice will vary between platforms, your key messages should remain consistent.



Use clear public language, get rid of mil-speak and consult your PA staff when in doubt.

Audience vs. Platform

	Facebook	Instagram	Twitter	LinkedIn	Snapchat	TikTok
Journalists						
Sailors & Families						
Local Community						
Veterans						
Partnership Nations & Allies						
Civilian Workforce						
Industry						
Academia						
Congress / HASC / SASC						
Potential Recruits						



Selecting the right voice for a given platform: People do their best work when they are interested in what they are doing. Though not required, a passion and interest in social media can hold the key to being effective in the space. Many times the most junior person is tossed the responsibility to “do social media”. This is not always the best approach. Though it is helpful to be a “social media native”, our recommendation is that you ask who has an interest in social and go from there. Those who have an interest will likely excel in the space and continue to innovate and try to find creative ways to communicate/connect with their audiences.



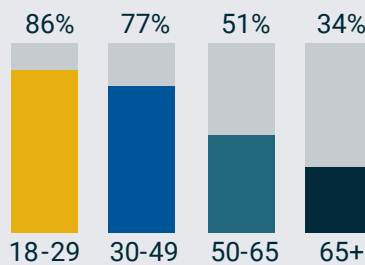
PLATFORM DEMOGRAPHICS

Generalities and platform by number. What are each platform's demographics and culture? These infographics will give you a sense of where these audiences live, you can better provide guidance to your team on where you would like to have a presence.

Facebook

Facebook is a social networking website where users can post comments, share photographs, and post links to news or other interesting content on the web, chat live, and watch short-form video and live event streaming. Shared content can be made publicly accessible, or it can be shared only among a select group of friends or family, or with even a single person.

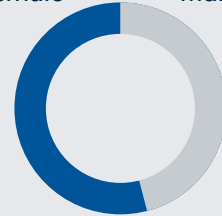
Percentage of People Who Use Platform, By Age



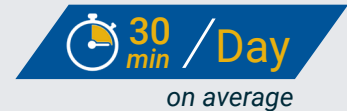
Monthly Users
2.9 Billion

By Gender

54% Female
46% Male



Time Spent

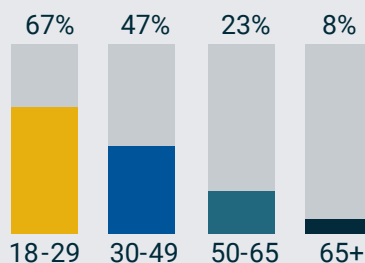


Demographics source: *The 2021 Social Media Users Demographics Guide* | Khoros

Instagram

A photo and video sharing app that has adapted to include an ephemeral content feature (modeled after Snapchat) called Stories and its newest feature Reels (modeled after TikTok). Instagram makes sharing really simple and includes a powerful hash-tagging system which allows users and brands to reach beyond their audiences and engage in broader conversations; as well as track against their own hash tagged content.

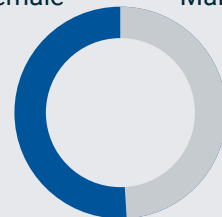
Percentage of People Who Use Platform, By Age



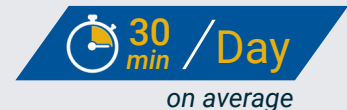
Monthly Users
1 Billion
Daily Users
500 Million

By Gender

51% Female
49% Male



Time Spent



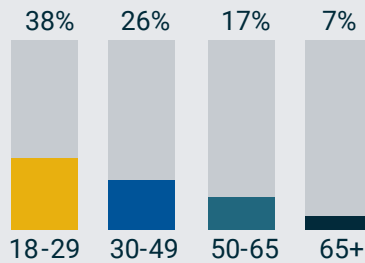
Most Followers



Twitter

An online news and social networking site where people communicate in short messages called tweets. Tweeting is posting short messages for anyone who follows you on Twitter, with the hope that your words are useful and interesting to someone in your audience. Another description of Twitter and tweeting might be microblogging. Twitter is the place to find out about what's happening in the world right now. Whether you're interested in music, sports, politics, news, celebrities, or every-day moments — Twitter enables you to see and join in on what's happening/trending now.

Percentage of People Who Use Platform, By Age

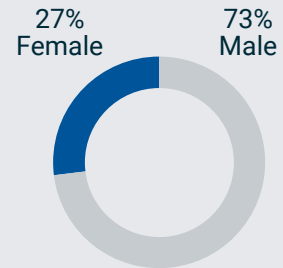


Monthly Users
436 Million

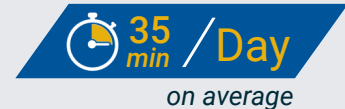
Most Followers



By Gender



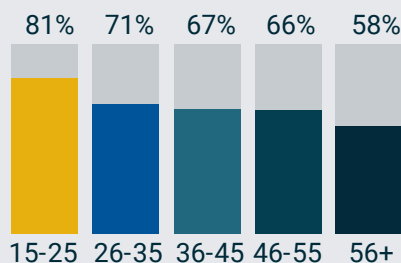
Time Spent



YouTube

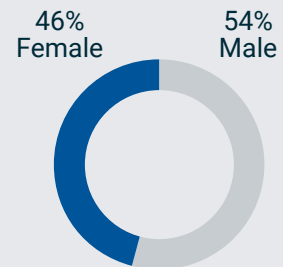
A free video-sharing website and the second largest search engine behind Google Search. All you need is a Google account to create a YouTube account to watch videos or create your own content.

Percentage of People Who Use Platform, By Age

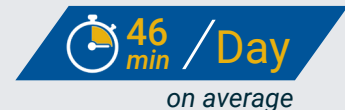


Monthly Users
2.6 Billion

By Gender



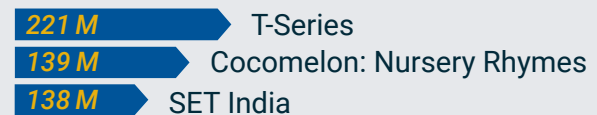
Time Spent



Additional Facts

- ★ 70% of views are on mobile devices
- ★ 1 billion hours of video is viewed each day
- ★ Available in 80 languages

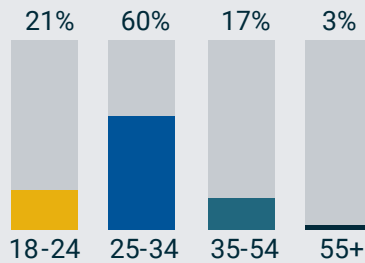
Most Followers



LinkedIn

Considered the social media platform for the working professional, young entrepreneur, or networking individual. LinkedIn users leverage job opportunities, connect with colleagues, and expand their professional network. Successful content on LinkedIn features thought pieces on technological advancements, inspiring anecdotes of success, and connecting like minded individuals in similar interest. LinkedIn currently has a less monetized algorithm than Facebook/Instagram/Twitter, therefore the organic reach is wider.

Percentage of People Who Use Platform, By Age

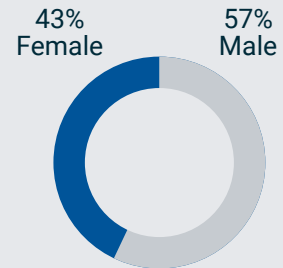


Monthly Users
90 Million

Most Followers



By Gender



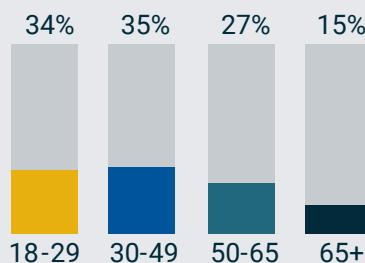
Time Spent



Pinterest

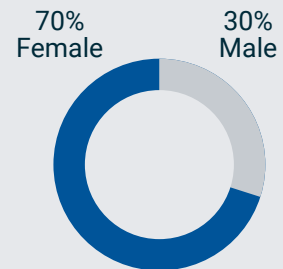
A visual discovery engine for finding ideas like recipes, home and style inspiration, and more. Your home feed is the center of Pinterest. It's where you'll find ideas, or Pins, with recommendations based on your interests, as well as what people you follow on Pinterest are saving.

Percentage of People Who Use Platform, By Age



Monthly Users
433 Million

By Gender



Time Spent



Additional Facts

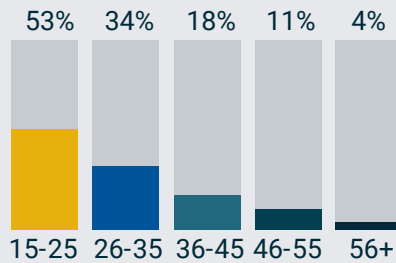
- ★ 90% of weekly pinners used Pinterest to make purchase decisions
- ★ Pinterest drives 33% more referral traffic to shopping sites than Facebook
- ★ People who travel are 2X more likely to use Pinterest



Snapchat

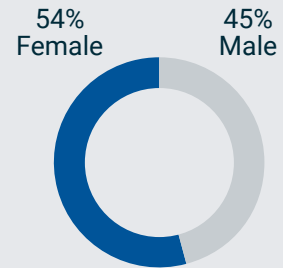
Both a messaging platform and a social network. It can't be used from a desktop and opens directly to a camera which makes it unique to other platforms. There is no feed or commentary. Just streams of ephemeral content, or moments in time that may be shared directly to another user to vanish or to your "story" for 24 hours. Snapchat is particularly popular amongst teens and young adults. A 2018 Pew report showed that 49% of Snapchat users visit the app several times a day.

Percentage of People Who Use Platform, By Age

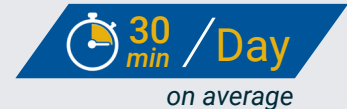


Monthly Users
557 Million

By Gender



Time Spent

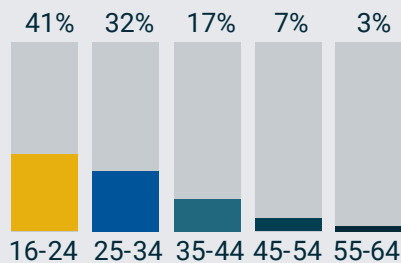


Twitch

A live-streaming platform for gamers and other lifestyle casters that supports building communities around a shared and streamable interest.

Twitch streamers "broadcast" their gameplay or activity by sharing their screen with fans and subscribers who can hear and watch them live. There are both free and paid versions of Twitch, with paid tiers removing ads and giving users access to more robust social, streaming, and storage features.

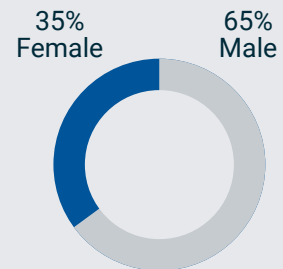
Age of Platform Users



Monthly Streamers
9.5 Million

Monthly Users
2.9 Million

By Gender:



Time Spent



Additional Facts

- ★ Twitch has market share of 67% content hours watched, and 90% of content streamed.

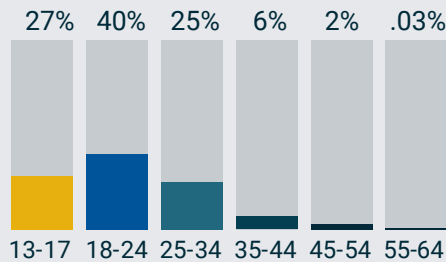


TikTok

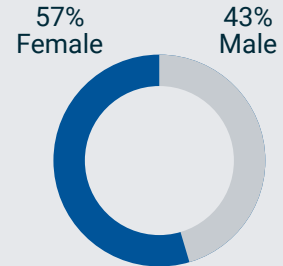
A short-form video sharing app with a feed that features an endless slew of micro-videos made by its users. Videos can be a maximum of 15 seconds long, with the option to combine videos for a 60 second long compilation. The app is known for its charming, often hilarious content featuring real people and real, home-made videos.

Currently not approved by DoD.

Age of Platform Users



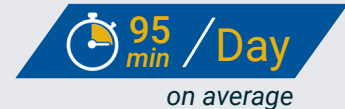
By Gender:



Monthly Users
1 Billion

Daily Users
50 Million

Time Spent



Additional Facts

- ★ 26.5 million monthly active users are from the USA
- ★ In less than 18 months, the number of US adult TikTok users grew 5.5 times.
- ★ 90% of TikTok users visit the app more than once per day
- ★ TikTok is available in 150 markets, in 75 languages
- ★ It's currently the third most downloaded non-gaming app of the year

Clubhouse

An audio-based social media app. The company describes itself as “a new type of social product based on voice [that] allows people everywhere to talk, tell stories, develop ideas, deepen friendships, and meet interesting new people around the world.”

This app allows users to gather in audio chat rooms to discuss various topics, whether it's sports, wellness, or Bitcoin. Rooms are usually divided into two groups: those who are talking and those who are listening (participants can see a list of everyone who is in a conversation, and the numbers sometimes run into the thousands).

Unlike Twitter, Clubhouse is a closed, hierarchical platform: A moderator oversees discussions and has the ability to let someone chime in or to kick out the unruly. In addition to the “clubs” sorted by topic, two or more users can join together and start their own chat room. Essentially, a podcast with audience participation.

Additional Facts

- ★ Clubhouse has over six million users, most of which were added in early 2021
- ★ Over ten million people have downloaded the app
- ★ Celebrities such as Elon Musk, Oprah Winfrey, Drake, Kevin Hart and Chris Rock have all hosted conversations on the app



Recommendations by Industry

	Facebook	Instagram	Twitter	Youtube	LinkedIn	Pinterest	Snapchat
Retail							
Media							
Sports							
Packaged Goods							
Financial Services							
Automotive							
Health Care							

Ideal for Industry
 Depends on Strategy
 Not right for Industry

Best Place for Teens
 Best Place for Millennials
 Best Place to Reach a Male Audience

Instagram + Snapchat
 Facebook + Instagram
 Youtube

Source: <https://khoros.com/resources/social-media-demographics-guide>

PLANNING CONSIDERATIONS

The Art of Storytelling

Times have changed, with new apps and trends popping up daily. But the art of storytelling remains the same. What makes a good story/a good storyteller remains the same. What elements of storytelling you already know can be applied to the social space? What mediums can you use to bring a story to life in an attention-grabbing and engaging way?

Social-First Planning

One thing that has changed is that communication has been flipped on its head. Where media used to lead the news cycle; with people posting and reposting what they share. The media is now finding much of their news on social media, retweeting and sharing or repurposing stories they find on Twitter or a story gone viral.

So how does that apply to our communication planning? Well, too often social media is an afterthought, an “oh yeah, can you put this on social media, too?” When looking at planning it is important to have social media in your initial consideration set. How (or will) this play in the social media space?

Example: Visuals. Let’s say a conference is planned and the day comes and 15 photos posted to Facebook of a person at a podium. This gets little to no engagement and falls flat because it’s not visually interesting or intriguing and because no one thought of the visuals or social media at the start of planning for that event. If social media is kept top of mind at the

beginning, interactive/experiential elements can be added to that conference — like a photo booth or interactive comment wall that grows on a time-lapse photo as people post stickies to a wall — or there are quote graphics pulled from the speech the speaker is to give that get scheduled and posted shortly after his/her portion concludes.

“ If a tree falls in a forest and no one Tweeted, Facebooked, Instagrammed, or posted a #TreeFallChallenge to TikTok . . . it didn't happen. ”

Approval Process

It is important to have a set of checks and balances within every social team so that we can check each other's homework and ensure mishaps do not occur.

Establish an approval process for your team that begins with creative discussion, goes through at least two sets of eyes for review — in instances of cultural products at minimum run by one person from that culture — and then a final approval stage that includes whatever level of staffing your command leadership is comfortable with. Keep in mind that contractors cannot be a release authority for content, therefore a uniformed service member or civilian must be available to review and approve planned content. Some riskier items or newer formats — memes and reels, may warrant extra scrutiny and lead time for those not familiar with the medium.

THE AGE OF THE INFLUENCER



What is an influencer? **One who exerts influence:** a person who inspires or guides the actions of others; often, specifically: a person who is able to generate interest in something (such as a consumer product) by posting about it on social media.

More and more, brands are beginning to rely on influencer marketing. That is, having someone with a large and/or engaged following in a given area carry your messaging for you to their own audiences in an organic way. These are usually paid partnerships but, with service branches, many influencers are willing to participate for brand equity alone.

If your team brings you a list of influencers they'd like to reach out to in order to amplify their message or event, here are some questions to ask:

1. Have they been vetted? That means has your team looked at their previous post history to ensure their feed isn't politicized one way or the other, that they have not posted anything derogatory with regard to the U.S. Navy, that they are verifiably who they claim to be.
2. Do their audience demographics include the audiences you are attempting to reach.
3. What level of influencer are they? What is their estimated reach? And do they have an organic tie to the subject matter being discussed or the U.S. Navy. Bigger isn't always better. Someone might have a very large audience, but not be a good brand fit; while



another influencer might have a smaller audience but in a very engaged niche that reaches the target and/or is better aligned to the messages you're wanting to convey and the U.S. Navy. Example: Smarter Everyday YouTuber paired with ICEX.

REGISTERING YOUR SOCIAL MEDIA PRESENCE

If you/your command decides on a social media presence it MUST be registered on Navy.mil and at www.digitalgov.gov/services/u-s-digital-registry

U.S. NAVY ACCEPTABLE USE REQUIREMENTS CHECKLIST:

Before beginning the registration process for the Navy Social Media Directory, please read thoroughly:

AN OFFICIAL NAVY SOCIAL MEDIA PRESENCE **MUST** HAVE:

1. Approval by:
 - Commanding officer or designated public affairs officer.
 - Someone with release authority for the command.
2. Acceptable Use Policy Acknowledgement (see appendix A)
3. The page name **MUST** closely match the command's name as displayed on Navy.mil's social media directory; this will also aid in page verification.

QUICK CHECK:

- Do not capitalize the entire page name. For example, USS ANY SHIP.
- Do not use "Page" in the title: Ex: "USS Ship Page".
- Do not use only an abbreviation. All social platforms are external facing and therefore, must account for non-military audiences.

Examples:

☒ Unacceptable: VFA-11

☒ Unacceptable: CVN-78

☒ Acceptable: Strike Fighter Squadron 11 - VFA-11

☒ Acceptable: USS Gerald R. Ford - CVN 78

4. Main POC must have a valid .mil address.
 - The only exception is for a command authorized to use .edu or .com. These commands should contact CHINFO directly for registration.
5. The page must link to the command's official .mil website.
 - If the command does not have a website, please use the ISIC's website.



6. The page must include the required disclaimers.
 - The disclaimer identifies the social media presence as an official Department of the Navy presence and disclaims any endorsement. (see Appendix B)
 - There must also be a disclaimer in the bio “following or liking ≠ endorsement.”
7. The presence must be set to public; not private and should be set up as a business page.
8. Two-step verification should be enabled to help ensure account security and linked to a mobile phone number for designated administrators or use a third-party authentication app. For instances on a ship, where connectivity may prohibit this, please ensure there is an admin ashore that can handle this requirement.
9. Adhere to strong password standards i.e. be 15 characters long, include upper and lowercase letters, numbers and at least one special character; AND be changed at minimum once a quarter as well as any time the account is alerted to compromise, or turnover of staff.

To add the required disclaimer on Facebook:

1. Click Settings on the upper right corner of the Facebook page.
2. On the left side of the Settings, click Page Info.
3. Under General Information, copy and paste the required disclaimer language into the General Information field. Replace the placeholder text with command specific information and click Save. The disclaimer template is available at **www.navy.mil/socialmedia** under digital media resources.
4. Go to **www.navy.mil/socialmedia**
Under Add Your Group, click Accept to submit the newly created page for registration.
5. The page will be reviewed for compliance with these registration requirements. The point of contact, which was used during the registration process, will be contacted to confirm registration or to address any issues that need to be corrected before the page is added to the Navy Social Media Directory.

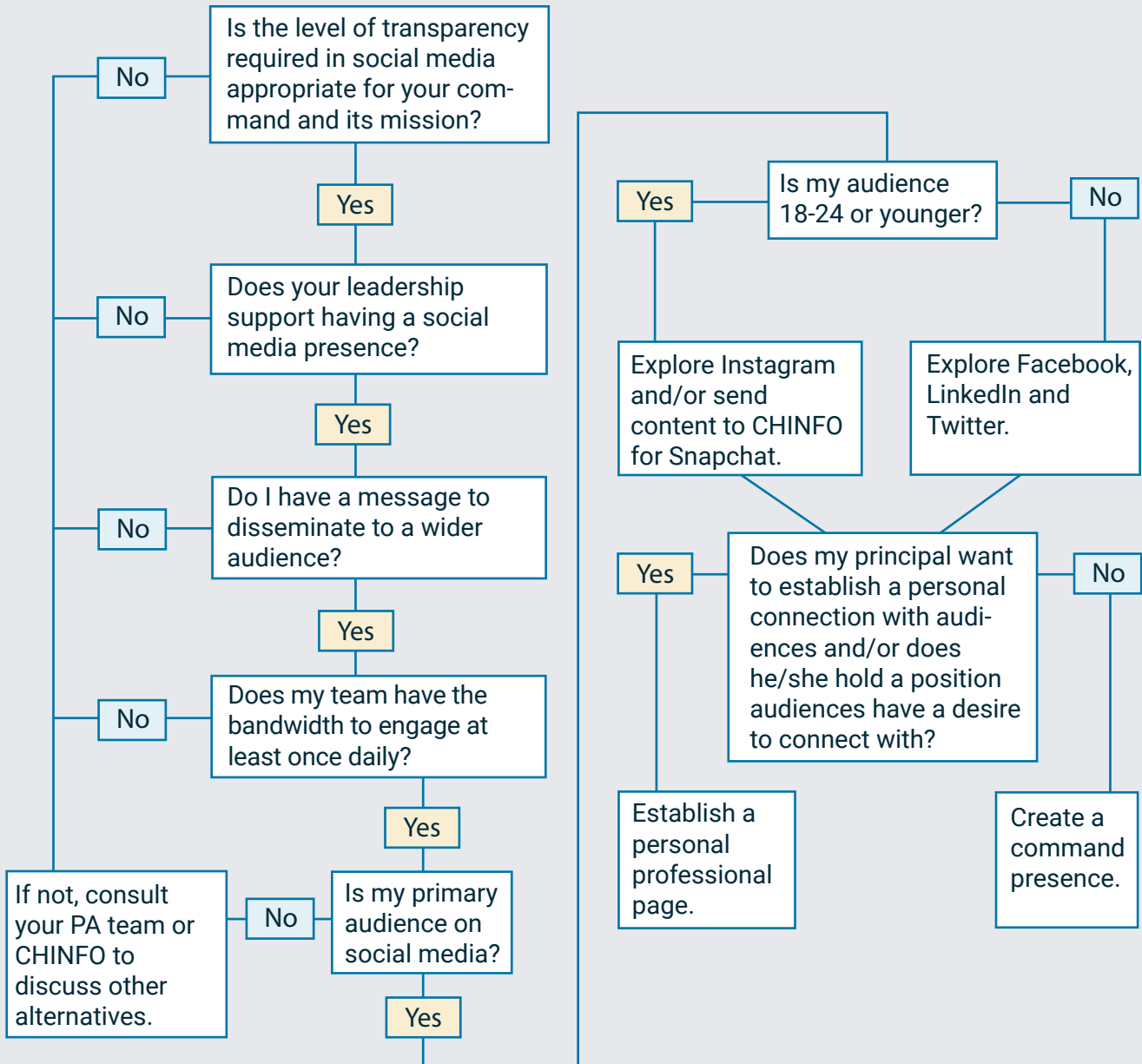


PLATFORM SELECTION

Where Should You Be? And Where Do You Start?

1. Should you engage on social media?

Decision Tree For Admins



2. Define your audience (See 'Audiences' section on this page). Who do you want to reach? What is your message?
 - The answers to these questions will tell you where you should be based on platform demographics and the type of information generally shared on that particular platform.
 - Determine where your efforts will have the most impact. You DO NOT need a presence on every platform. Do not feel that you must use multiple platforms. It's far better to have one successful social media site than multiple sites that aren't used effectively.
 - You must also keep in mind what is sustainable given your staffing. Do you have the content and personnel — both now and long term — to routinely engage with priority audiences?
3. Once you determine which platforms you will engage, it's time to create your presence.
 - Create an account as a business versus a personal page. This will give you access to better analytics.
 - Create your account with a centrally accessible account to which your team has the password. This will make it easier to deal with two-step verification and password changes when there is personnel turnover.
 - Ensure you protect your account with a strong password and link to a government mobile phone number that makes sense given your structure and has texting capability. Passwords should be changed at least quarterly and include uppercase, lowercase, numbers and special characters; as well as utilize two-step verification using a government cell phone number.

AUDIENCES

Who Are You Talking To? Where, How and About What?

1. Build a profile (persona) for whom you are talking to on each platform and the distinct voice you will use to speak to each.
 - What are they interested in? What should they know?
2. Include a 'Tone and Voice' section that speaks to what your voice will be on each platform. For example: The tone and voice on Instagram may be snippy, playful, and informed, whereas Facebook is more formal.

A helpful exercise can be to create a persona for a fictional individual in the group you wish to target. For example. . .



User Personas

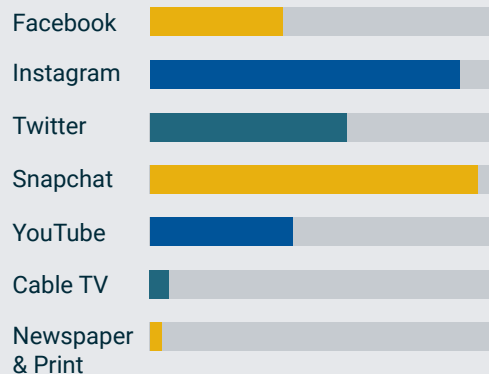


Age/Generation 18 / Zoomer
Occupation High School Student & Cheerleader
Location West Coast
Archetype Heading to college

Amazing Amy

Amazing Amy hopes to make the cheerleading squad at the collegiate level while maintaining her scholarship GPA and acquiring a degree in Physical Sciences. She has little to no connection to the Navy but knows that we have one. She uses Instagram to build her personal brand and connect with friends and keeps a Facebook just to correspond with her family members on Messenger.

Media Activity

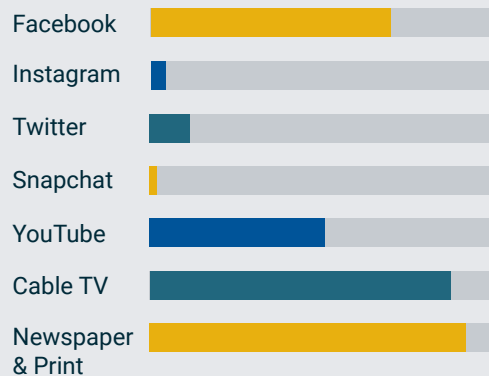


Age/Generation 60+ / Boomer
Occupation Retired
Location Southern US
Archetype Navy Veteran

Grandpa Eddie

Grandpa Eddie aspires to see his grandkids once per quarter at minimum and to be the "cool grandpa" by communicating with them via Facebook messenger. He communicates with other Veterans and old shipmates via Facebook groups. He shares photos of his kids' families and voices his opinion on Navy platforms. He likes to travel and has two trips planned overseas this year in areas where COVID restrictions are lifted.

Media Activity

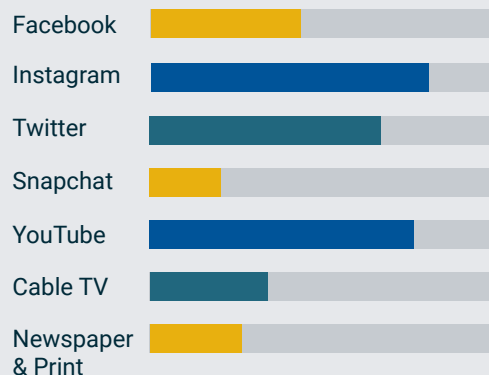


Age/Generation 30's / Millennial
Occupation Manager
Location Midwest
Archetype Small-town guy

Casual Carl

Casual Carl spends most of his social media time on YouTube. He uses Facebook and Instagram to communicate with friends and family. His major goal this year is to marry his long-time girlfriend and begin a family as he has just received a promotion at his job in cyber. When he is on social media he mainly scrolls for funny videos. He rarely shares anything, but keeps abreast of news feeds via Twitter.

Media Activity



Source: <https://gonavy.xtensio.com/nm8na8bo>

See the Appendix for a blank, printable version.








SETTING GOALS & OBJECTIVES

What Is Your Overarching Communication Goal?

What are your yearly, monthly, weekly and daily communication objectives to reach that goal?

Objectives:

When writing objectives, remember to make them specific, measurable, realistic, relevant to your goals, and achievable within a realistic time frame. For quick reference, see the chart below.

S	Specific	Make your goals specific and narrow for more effective planning.	
M	Measurable	Define what evidence will prove you're making progress and re-evaluate when necessary.	
A	Attainable	Make sure you can reasonably accomplish your goal within a certain timeframe.	
R	Relevant	Your goals should align with your values and long-term objectives.	
T	Time-Bound	Set a realistic, ambitious end date for task prioritization and motivation.	

Source: <https://www.indeed.com/career-advice/career-development/smart-goals>

Example Objective:

Publish content that increases understanding of the Navy with external audiences and makes the Navy relevant to their lives and what they care about resulting in better positioning in the market among other services per various survey results, by the end of Q1.

Engage younger Gen YZ demographics to expand reach beyond internal audiences.

Engage women particularly in the 18-24 demographic.

Key Performance Indicators (KPIs)

Once you have your goals and objectives, you must determine what metrics you will track in order to measure how you are doing towards them.

What variables will you look at to indicate the success of your content?



Here, turn your goals into metrics you can measure. Examples: views/impressions, shares.

- X increase in followers by the end of Q1.
- X increase in reach per by the end of Q1.
- X number of engagements by the end of Q1.

How will you measure them? What measures are important to your leadership?

Select Key Performance Indicators (KPIs) to routinely track in order to gauge the above.

Example:

Primary KPIs:

5% Increase in X metric (subscriptions to your e-newsletter, for example).

Audience Reach:

16-24 demographic: Increase followership of 2% quarter over quarter on Facebook and Instagram.

Increase in the percentage of women across platforms by 1% quarter over quarter.

Audience Engagement:

Aggregate increased engagement (likes/comments/shares) across platforms 2% quarter over quarter.

50% increase in response rates.

Secondary KPIs:

Unique website visitors to website.

KEY CHANNELS

Next determine on which channels you will communicate to achieve the above and how you will utilize each one.

Example:

1. Owned Social
 - US Navy Facebook/Twitter/Instagram/Snapchat/Pinterest/YouTube
 - Fleet Accounts/Recruiter Pages
2. Social Influencer (Internal/External)
 - Page Posts/Mentions
 - Shares



3. Traditional Media
 - News Coverage
 - Associated Social Posts
4. Paid Media – While we do not participate in paid media in Public Affairs, we should look for opportunities to capitalize on marketing/recruiting buys by aligning messaging with CNRC where possible.
5. Web
 - Navy.mil resources: Blogs, Photos, Video, News.
6. Outreach Events
 - Leverage social media influencers to make events more impactful with regard to reach. Whereas having traditional media in attendance may yield an article, having a YouTuber, Twitch Streamer, or Instagram/TikTok influencer in attendance may pay dividends in reaching particular segments. Example: A tech influencer at the unveiling of new Navy technology.
7. Defense Visual Information Distribution Service (DVIDS)
 - Submit content natively to DVIDS to increase collaboration and timely use of content across the DON digital enterprise.

Key Channels

	Demographic	Content	Voice	Where to Submit Content
Facebook	35+, largely internal, parents, traditional influencers and supporters	Photos, videos, story links	Personal	Self-publish, flagged for sharing
Twitter	35+, adversaries	Timely news and info, story links and photos	Professional news	Flagged for retweet
Instagram	Gen YZ	Intriguing visual content, vertically shot video for IGTV and stories	Young sailor, funny, upbeat	Self-publish, flagged for sharing
Navy.mil	All publics, largely internal	Timely news articles, photos and video	Professional news	Send content to CHINFO for native publishing
YouTube	All publics, largely external	Engaging video content, longer form, 3+ minutes, episodic	Varies	
Pinterest	Women	Interesting visuals and aspects of the Navy, How-to's, linked photos	Engaging, descriptive, conversational	
LinkedIn	Business Professionals	Industry articles, career information, military and civilian	Professional, authoritative	
Snapchat	Gen Z	Takeovers by leadership, Sailor generated, vertically shot	Positive, open, engaging	
Twitch	Gen YZ	Live-streaming video, podcasts	Informative, real, engaging	

See the Appendix for a blank, printable version.



CONTENT PLANNING

What Will You Share? And When?

1. Start by creating themes for each month and/or nest with CHINFO themes tying your specific command messaging in with broader Navy messaging themes (See Appendix. Sample Calendar.) Once you have your desired themes and key messages laid out for each month it's time to build your calendar.
2. Planned Events: Take a look at your organizational calendar. What events, speeches, special anniversaries (Navy Birthday, for example) do you want to share with your audience(s)?
 - Are they interesting for your audience(s)? If not, how do you tell that story in an engaging way? For example, if it is a speech, what quotes can you pull to make a graphic? If it is video, what kind of treatment will catch attention in six seconds or less?
3. Ad-hoc Events: Retweets/Shares of relevant content, (from fleet/flagship/DoD pages or relevant and vetted influencers), command updates, COVID policy updates, accomplishments, media coverage etc.
 - Save room in your calendar for these as they emerge. Perhaps pick one time of day that you can keep open for anything that may help with a broader message.
 - Again, how do you tell these stories? Experiment with days/times/formats to see what works for your particular audience.
4. Yearly Social Media Days and Holidays: Join conversations like Fitness Fridays and dates such as "National Siblings Day" using their associated hashtags (#FitnessFriday #NationalSiblingsDay). Look at a social media calendar online or at the Navy's social media calendar at www.navy.mil/socialmedia to see what works/aligns with your organization organically. For example, "National Basket Weaving Day" probably would not work for your organization. But "National Pet Day" might. This is where a little creativity can go a long way to reach audiences that do not currently follow your page and/or care about the Navy. Although they might seem silly to some, they are a proven way to reach new audiences and tie to a broader conversation in a tangible way.

Content Examples



Fitness Friday



National Siblings Day



Christmas



Coffee Day

Source: Instagram@USNavy



Content Examples



Virtual Fleetweek



World Emoji Day



Star Wars Day



Chocolate Day

Source: *Instagram@USNavy*

5. Interaction with Influencers: Every once and a while you will notice a celebrity or influencer tag you or your organization, or more likely, the flagship Navy page. In these cases, depending on what is said, and how it's said you may interact with their account with great benefit, **ONLY** if you can check the following two blocks:
- ☒ You review their social pages to ensure there is no inflammatory, racist, extremist, high profanity content or content that would otherwise reflect badly upon the Navy.
 - ☒ You inform your leadership before you interact. (This is so that they are prepared should anything generate news by your interaction.)



What is an influencer? **One who exerts influence:** a person who inspires or guides the actions of others; often, specifically: a person who is able to generate interest in something (such as a consumer product) by posting about it on social media.

6. Trending Topics: We are all aware of “trending” topics and memes, stories, videos that go “viral” and probably share some understanding that tapping into those as they happen can expose your content and presence to audiences who likely would not otherwise see it, as well as provide a bump in followership and more importantly engagement. But how do you tap into these effectively?
- Know your audience. For example, brands tend to post memes and have a little more “fun” with communications on Instagram where the audience is younger and more accepting versus other audiences may not share the same sense of humor nor understand certain trends.
 - DO NOT meme just for the sake of memeing. There must be a communication objective and a clear and organic tie to your organization/brand. If not, it will not resonate and may be seen as amateurish.



Memes Examples



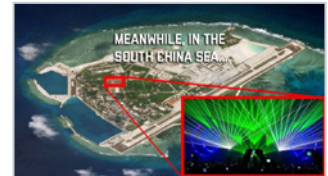
USS Constellation



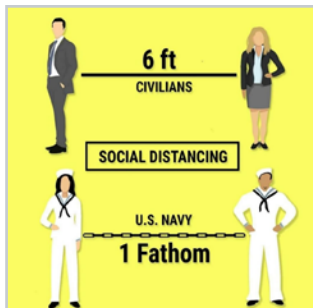
Greyhound Premiere



Incident in South China Sea



Incident in South China Sea



Social Distancing



Hand-washing Techniques



Waiting for Top Gun 2



Urban Outfitters Selling Navy Coveralls

Source: Instagram@USNavy

CONTENT MEDIUMS

What kind of content do your audiences engage with? Try different forms of content and do more of what works and/or tie into social media trends e.g.:

1. News Articles
2. Interviews
3. Blogs/Podcasts
4. Memes and GIFs
5. Navy photos (carousels, photo galleries)
6. Navy Trivia Questions #TriviaTuesday
7. Navy Videos: Testimonials, Infographics, Tutorials, Episodic content.
8. Vertical Video, Episodic content (IGTV/stories, Snapchat) putting credits or slates at the end of videos.
9. Special Occasion Posts (Cultural months, holidays, etc.)



10. Instagram Stories

11. Sailor Influencer content: Build relationships with our Sailor-influencers within your fleet and/or external influencers with a narrative/brand that ties to the Navy or elements of the Navy; and create content with them with the intent for them to share on their own platforms to increase reach and engagement. Remember to provide ground rules to make sure Sailors are not profiting financially by their engagement.



As you post, be aware of internal and external trends.

- What type of content works for which platform based on your analytics? Do more of what works and less of what doesn't.
- What is trending externally – conversations, topics, hashtags, meme formats – that you can tie into organically?

CONTENT CREATION & DISTRIBUTION

1. Your content – stories, photos, videos (b-roll and productions), infographics (still and video), blogs, etc. – is needed to tell our Navy's story. Submit content to the Navy.mil content management system and then amplify on your social media platforms.
2. Flag campaigns and content for CHINFO for greater amplification. In order to do so, simply send an MS Teams message with a link to the post in the weekly Social Media Lead Huddle channel or email **NavySM@us.navy.mil**
3. Encourage fleet participation.
 - If you identify microinfluencers with followings of 300+ within your command; ask them to share content, do a takeover, or host a Q&A on your platform; or flag them to CHINFO for a takeover inclusive of your messaging on big Navy platforms.
 - Ask your Sailors to tag content they would like considered for sharing on big Navy platforms to tag their content with **#ShareMyNavy** on Instagram.
4. Don't stop your own greatness. If you have a creative idea, SHARE IT. The worst that can be said is "no" and even then, tweaks can be made to get to "yes". SHARE IT. (The Navy Social Media Fo'c'sle Group on Facebook is great place to share your ideas in an open and creative environment.)



BEST PRACTICES PER FORMAT/PLATFORM

For All Platforms

- ✓ Use plain language. Whether you're writing a story, release, caption, or post — work to ensure an external audience with little or no interaction with the Navy can understand what you're wanting to convey. How would you explain a photo or Navy concept to a friend of yours who has no connection to the Navy?
- ✓ If you make a mistake, do no attempt to cover it up. Just own up to it and humanize your platform. Everyone makes mistakes. The best thing to do if someone points out a mistake is acknowledge and let them know you've fixed it (Facebook/Instagram) or post the correction in the comments if you're on Twitter where post editing is not an option.

Navy.mil Articles

- ✓ Ensure you have a headline/lead that grabs attention.
- ✓ Avoid the use of acronyms.
- ✓ Use AP Style.
- ✓ Include good quotes that can be pulled for social media amplification.
- ✓ Include an impactful visuals [photos, graphics and video] captions.

Navy LIVE Blogs:

- ✓ Speak in first-person voice.
- ✓ Be conversational versus newsy.
- ✓ Make it personal.
- ✓ Include impactful visuals.

Facebook:

- ✓ Photos and videos perform the best.
- ✓ Videos uploaded natively work the best and garner the most reach.
- ✓ Like comments and reply where appropriate in a conversational tone; Facebook's latest algorithm rewards organic conversation happening in the comments.

Twitter

- ✓ Use relevant hashtags/tags; no more than three per Tweet as a rule.
- ✓ Keep it short.
- ✓ Include embedded photo caption.
- ✓ Post short form video.
- ✓ Use Twitter tools i.e. polls; not to collect PII or demographic data, but for "fun" topics and interests in order to engage the audience.



Instagram

- ✓ Use impactful visuals.
- ✓ Upload videos into Instagram TV (IGTV). Keep videos between 90 seconds and 3 minutes.
- ✓ Utilize stories. Stories pull people into your page. Utilize all stories' features. Mix it up to keep it fresh.
- ✓ Utilize the new REELS feature which is Instagram's answer to TikTok and shares a lot of the same functionality.
- ✓ Use relevant hashtags to pull you into other feeds and make your content discoverable to a wider audience.

Capturing Video for Stories and Snapchat

- ✓ Shoot vertically in the platform; or shoot horizontally, but wide enough so that it can be cropped for vertical storytelling later.
- ✓ Get close to your subject: Medium close-ups are ideal for capturing the best composition and audio.
- ✓ Don't be afraid to let the subject hold the phone and speak to it. This gives the audience a sense of connection.
- ✓ Pick an interesting background: Try to shoot your talent in front of a background that is relevant to your topic/theme.
- ✓ Tell a COMPLETE visual story.
- ✓ Stabilize your shot: Use a tripod or place your camera/phone up on the surface (table, chair, shelf, etc.) if possible. If you have to shoot handheld make sure to enable camera stabilization on your phone.
- ✓ Avoid backlighting (e.g. light source placed behind your subject).
- ✓ Audio matters: Place your camera/phone as close to your subject as possible (while still following tip #2) so the dialogue is captured clearly. Listen to the audio after shooting to make sure everything was captured cleanly.

Snapchat

- ✓ @usnavy Snapchat is intended to be an aggregator of stories from across the fleet. This is the best practice on the platform and has resulted in much success for the Marines.
- ✓ Please send your content to CHINFO.



Channel Optimization

Platform	Frequency	Optimal Times
facebook.com/usnavy	1-2 times per day	9am, 12-3pm, 8-9pm
instagram.com/usnavy	1-2 times per day	7-9am, 11am-1pm, 7-9pm, 2am
youtube.com/usnavy	1 time per week	2-4pm MTW, 12-3pm ThF
twitter.com/usnavy	10-15 times per day	6-8am, 1-3pm
snapchat.com/usnavy	2 times per month	10pm-1am
pinterest.com/usnavy	11 pins per day	8-11pm
linkedin.com/usnavy	2 times per week	10-11am TWTh

See the Appendix for a blank, printable version.

*** These reflect (generally) the best times/frequency per latest information on algorithms and when the largest audience is online. *That said, the BEST information for your respective audiences is found in your platform insights which show the optimal posting times for your particular platforms.*

CRISIS COMMUNICATION

No matter the origin of a social media crisis, it is important to be prepared. In the age of misinformation campaigns from our adversaries, quick, well-orchestrated action can mitigate the potential for negative impact to the Navy's reputation. It is also important to remember that reactionary action can fuel or exacerbate crises.

Therefore, having a crisis communication plan in place is essential. Therefore, having a social media crisis communication plan in place, where the news of crises usually hit first, is essential. Your social media crisis comm plan should nest within your commands overarching crisis communications strategy.

Your first step should occur before the crisis: ensure your team/command/families know how to identify a potential or brewing crisis and who they need to inform. It is important to establish in a crisis situation who is really responsible for responding and who needs to be informed. This will vary widely if the crisis is one of misinformation or if it is something more kinetic like a natural disaster or a law enforcement issue. Start by identifying who your primary and secondary leads will be during a crisis and ensure you have shared after hours contact information for them.



Please include as part of your plan alerting CHINFO if you notice an uptick in comments on your platforms regarding a particular issue or post and/or if there are any other areas of concern.



What is an online crisis? *Online chatter that indicates potential for a large negative impact on the reputation of the U.S. Navy as an institution and brand; either within your physical area of operation where lives may be at stake or online.*

See Something, Say Something

Community managers across the fleet should immediately alert the CHINFO OI-3 News Desk at **703-697-5342** and email OI-2 at **NavySM@us.navy.mil** whenever they see suspicious activity in their engagement queues.

AREAS OF POTENTIAL RISK

Security

This category covers situations that occur on an owned property, either physical or digital, that have the potential to go viral online:

- U.S. Navy social media accounts hacked.
- Navy.mil hacked.
- Physical location threat.
- Personal, including leaked PII and high-impact catfishing.
- Cybersecurity issues.
- Local or national terrorism including attacks from fundamentalist groups.
- Impersonation of Navy leadership.

Negative Media Coverage

This category covers negative media coverage that leaks to social media as well as tactics by media to develop stories based on social posts.

- A negative or factually inaccurate article, coverage, or op-ed that gains traction on social media.
- Articles expected to post that could have widespread negative implications if it spreads on social media.
- Comments from reporters on a negative post wherein the reporter seeks more information from the original author for a news story.
- A reporter soliciting negative stories on social about the Navy for an article.
- When a person tags the media in a negative post about the Navy they would like to see published or investigated by the media.

Example: This U.S. Army tweet ultimately resulted in an article in *The New York Times*, *Time*, NPR, and Slate.



Non-Core Values/Sailor Issues

This category includes posts and comments that directly showcase poor behavior in current Navy personnel that could negatively impact sentiment, whether posted by the Sailor or by others highlighting values that do not reflect honor, courage, commitment.

- Content from Sailors that is culturally insensitive.
- PII or classified information shared by Sailors on social channels.
- Allegations of sexual assault or other crimes creating a large negative impact.
- Allegations of hazing.
- Content that indicates bias, prejudice, sexism, racism or extremist views.
- Suicide ideations.

Political

This category includes posts and comments from influential political figures, as well as political news.

- Partisan tweets from key politicians about topics that could impact the Navy's image.
- Partisan tweets from social media influencers or celebrities that could impact public perception of the Navy.
- Negative opinion pieces in key media outlets.
- Election-based posts that reference the Navy.
- Legislative moments in time.
- LGBTQA issues related to the Navy.
- Immigration issues related to the Navy.

INDIVIDUAL RESPONSIBILITY

Individual responsibility online is a SHARED responsibility. We all play a part in putting our best foot forward in representing our Navy as well as securing its operations and most importantly the safety and well-being of all.

Online Behavior

Rule of thumb: If you wouldn't tag your boss or Sailor's boss in a post due to its content, you probably shouldn't post it. Keep in mind — rightly or wrongly — any time you post a photo of yourself in uniform, you immediately become a spokesperson for the entire Navy in the eyes of the external audience. Anything you post, no matter how small your audience can become viral in a matter of seconds.

It is also important to note that just as with physical misconduct offline, misconduct ONLINE is also subject to UCMJ. Scary thought, we know. However, this does not mean you are discouraged from engaging. On the contrary, engaging on social media in a positive way; representing yourself and the Navy well, serves to carry the Navy story to the American public



and others and gives you an opportunity to tell your own story.

Consult with your immediate supervisors when you have questions.

Deputy Secretary of Defense Policy Memorandum, Hazing and Bullying Prevention and Response in the Armed Forces, Dec. 23, 2015:

Identifies **hazing** as so-called initiations or rites of passage in which individuals are subjected to physical or psychological harm. It identifies **bullying** as “acts of aggression intended to single out individuals from their teammates or coworkers, or to exclude them from a military element, unit or Department of Defense organization.” Additionally, the memo states that hazing and bullying are *unacceptable and prohibited* in all circumstances and environments, including off-duty or unofficial unit functions and settings, as well as on social media and other digital environments.

Also, **intimate images taken without consent**, or posted online without consent constitute *violations of the UCMJ and Navy Regulations*. As outlined in the CNO’s Design for Maintaining Maritime Superiority core attributes, the Navy is a values-based organization where everyone is expected to conduct himself or herself in a manner that is “**always upright and honorable, both in public or when no one is looking.**”

THE UCMJ & NAVY REGULATIONS

When online, to include social media, Sailors are subject to the **UCMJ and Navy regulations**, *even when off duty*. Commenting, posting or linking to material that violates the UCMJ or Navy Regulations may result in administrative or disciplinary action, including administrative separation and may, subject civilians to appropriate disciplinary action. Punitive action may include Articles 88, 89, 91, 92, 120b, 120c, 133 or 134 (General Article provisions, Contempt, Disrespect, Insubordination, Indecent Language, Communicating a threat, Solicitation to commit another Offense, and Child Pornography offenses), as well as other articles, including Navy Regulations Article 1168, non-consensual distribution or broadcast of an image.

Behaviors with Legal Consequences

Electronic harassment

47 U.S.C. § 223 (a)(1)(C) makes it a crime to anonymously use a telecommunications device (i.e. telephone, computer, or other electronic devices used for communication) to harass a person; 47 U.S.C § 223 (a)(1)(E) prohibits initiating communication via a telecommunications device solely to harass the recipient.

Electronic threats

18 U.S.C § 875 prohibits transmitting communications containing threats to kidnap or physically injure someone. It also criminalizes the actions of someone who, with intent to export (receive anything of value), electronically threatens to injure the property or reputation of a person. Sextortion (being tricked into providing sexual images and then being asked for money to not have the images published online) may fall under provisions of this law.

Cyberstalking

18 U.S.C. § 2261A prohibits a person, with the intent to kill, injure, harass, or intimidate



someone, from using a computer (or other digital communications system), to engage in actions (course of conduct) reasonably expected to cause a person (or immediate family member, spouse, or intimate partner) substantial emotional distress.

Obscenity

47 U.S.C. § 223(a)(1)(A) prohibits using a telecommunications device to make, create, or solicit and transmit any obscene comment, request, suggestion, proposal, image, or other communication.

Child exploitation / Child sexual exploitation

18 U.S.C. § 2251, 2252, and 2252A. Using a computer (a smartphone is a computer) to solicit, make, create, transmit, or receive child pornography is illegal. For these provisions, a child is anyone under the age of 18. 18 U.S.C. § 1462 makes it a crime to transmit obscene matters. 18 U.S.C. § 1470 criminalizes the transfer of obscene materials, including digital images, to persons under the age of 16. **Sending sexually explicit (graphic dirty talk) electronic messages to minors, or soliciting sexually explicit communications, also are criminal offenses.**

Computer misuse (hacking)

A person engaging in cyber misconduct may also commit violations of 18 U.S.C. § 1030, if, for example, he or she exceeds authorized access to the computer or accesses the computer without authorization (i.e. hacks into an account or network) to send harassing, intimidating, humiliating, or even threatening communication.

Extremism

NAVADMIN 044/21 covers the Navy's policy on Extremism in the ranks:

"Extremist behaviors and conduct, even if from only a small percentage of our force, violate our Core Values, are detrimental to good order and discipline, reduce warfighting readiness and degrade the toughness, trust and connectedness we are building in our Sailors and teams through our Culture of Excellence campaign.

Service members and civilian personnel must clearly understand the damaging effects of extremism and begin developing more effective, sustainable ways to eliminate the corrosive impacts extremist activity can have on our Force. As public servants, we took an oath to the Constitution and we will not tolerate those who participate in actions that go against the fundamental principles of the oath we share, particularly actions associated with extremist or dissident ideologies. Service members, Department of Defense civilians and all those who support our mission, are entitled to an environment free of discrimination, hate and harassment."

Speech in the workplace that interferes with the mission, espouses extremist or discriminatory doctrine, or is disrespectful and harmful to colleagues, will have consequences.

Extremism Training and resources: <https://go.usa.gov/xtsc8>

Reporting Incidents

Reporting Incidents Any member of the Navy community who experiences or witnesses incidents of improper online and/or extremist behavior should promptly report it to their chain of command via the Command Managed Equal Opportunity manager or Fleet and Family Support office.



Additional avenues for reporting include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices, and Naval Criminal Investigative Service.

*** NCIS encourages anyone with knowledge of criminal activity to report it to their local NCIS field office directly or via a web or smartphone app. Specific instructions are available here: <https://www.ncis.navy.mil/Resources/NCIS-Tips>

Rules of the road for our Sailors, Families and Navy civilians online:

- When you are online, you are in public — so act like it.
- Do not do or say anything online you would not do or say in public.
- Keep relationships and personal life private; setting your page to private is a good practice.
- There is no such thing as complete anonymity online (even if your page is private).
- Before you post, STOP and THINK.
- Words matter and can be taken out of context.
- Images can be taken out of context.
- Cool off before responding to messages in anger.

Anyone anywhere can see what you post. The internet doesn't forget. All it takes is a screenshot or download of an image to make sure one moment online lasts an eternity. Anything shared online, although intended to be private and confidential, has the possibility to become public — if it is best left unsaid, do not say it. If you do not want it shared, do not post it.

Protect your privacy and your friends' privacy too by not sharing without their permission. And unless you are prepared to attach that post, text, or photo to your next security clearance package, or resume, again, do not post it.

Anything posted on the internet is permanent. Through the use of publicly available online tools, data can be recovered and used against you.

OPSEC and Identity Management Concerns

We've all heard the phrase "practice good OPSEC" — but what does that mean in the social space? The same thing it has always meant. The same information that can be collected and pieced together by adversaries in person, can be done so more swiftly and easily via social media. Be careful not to post movements, deployment dates, ship dates (if you are a new recruit), when your spouse or parent is gone or coming home (if you are a Navy spouse or dependent). If you wouldn't share it with a complete stranger in person, do not disclose it to complete strangers online. Even if your page is "private" there are ways for bad actors to acquire information.

What is Identity Management?

Identity management (IdM), also known as identity and access management (IAM) aims to ensure that ONLY authorized people have access to the technology resources they need to perform their jobs. It includes policies and technologies that encompass an organization-wide process to properly identify, authenticate, and authorize employees based on their identities.



Identity management has gained importance over the past decade due to the growing number of global regulatory, compliance, and governance mandates that seek to protect sensitive data from exposure of any kind.

Take your identity and your personal brand seriously. Report fake profiles of yourself, leadership, or others you may know to the platforms themselves and flag them for CHINFO staff if the page(s) are not taken down or taken to resolution. In the same way you protect your credit, CAC card, social security number and other personal information; be careful what you share about yourself online. Is your birthday, or other PII displayed on your profile? Make sure to check your page from another browser or account in order to see what your profile actually reveals to other and then fix your profile settings accordingly to ensure you are not revealing more about yourself than you'd want a stranger to know. A lot can often be gleaned from profiles even when they are set to "private".

BOTS

Knowing whether an account is a bot or troll pretending to be an actual person is difficult. By some estimates, a quarter of all social media accounts may be bots and/or inauthentic accounts. Bots have been used by foreign governments, private companies, and terrorist organizations.

Some are controlled by an AI, others are controlled in what are often referred to as "troll farms", places where real people are paid to use dozens to hundreds of fake accounts online to pose as real people, usually using stolen identities. These types of accounts are sometimes referred to as "sock puppets".

If you come across a tweet and are not sure if it is from a bot, here are some things you can do to assess whether it is a bot or a real person:

1. Check for account verification. If there is a check mark next to the account name, then it has been verified to be a real person or organization by the site.
2. If there is no check mark: Check the handle of the account. Fake accounts often contain a lot of random numbers or letters in the handle (i.e., RealPatriot274hg6yt).
3. Look at the age of the account. If an account is around or less than a year old, it could likely be a bot. If the account is years old, but only appears to have started tweeting, posting, sharing etc., within the past few months, it is also likely a bot. Many bad actors will create hundreds of accounts with the intent of keeping them quiet for a couple years to try and escape detection.
4. For Twitter you can use a free open-source tool called Bot Sentinel:
 - Go to <https://botsentinel.com>
 - Click on "Analyze Account" in the top left on the main page.
 - Paste the account handle and hit "submit". It will then go through all the Twitter activity of the account and give it a grade on a scale of 0 to 100 on the likelihood that it is a bot or a troll. Generally, it is a good idea to assume it is a fake account if the score is 65 or over.



GUIDANCE

Page Registration and Acceptable Use Policy

- All official Navy presences are required to register on Navy.mil

Account security

- Passwords should contain both Upper and Lowercase, numbers and special characters and be 12-16 characters long.
- Change passwords at least quarterly.
- Enable two-factor authentication using your phone number or 3rd party authentication app to help ensure your account stays secure.
- Only add/ allow people you know to follow you.
- Set your page to “private” for an added layer of security
- Report fake profiles in your likeness, Navy leadership, or others to the platform via their reporting options. If it is not resolved, report it to NCIS and/or alert CHINFO OI-2 at **NavySM@us.navy.mil**

Records Management

- NARA Bulletin 2014-02 provides guidance on managing social media records.
- Social media allows individuals to collaborate, create, organize, edit, comment on, combine and share content, likely resulting in the creation of Federal records. The Federal Records Act (44 U.S.C. 3301) defines Federal records as any material that is recorded, made or received in the course of Federal business, regardless of its form or characteristics and is worthy of preservation. Social media content that meets this definition must be managed according to the applicable laws and regulations.
- The statute and its implementing regulations place responsibility with each agency to determine what Federal records they create or receive. Refer to 36 CFR, Chapter XII, Subchapter B, for guidance on how agencies should apply the statutory definition of Federal records.

The following non-exhaustive list of questions will help agencies determine record status of social media content:

- Does it contain evidence of an agency’s policies, business, or mission?
- Is the information only available on the social media site?
- Does the agency use the tool to convey official agency information?
- Is there a business need for the information?

If the answers to any of the above questions are yes, then the content is likely to be a Federal record. Also, social media content may be a Federal record when the use of social media provides added functionality, such as enhanced searchability, opportunities for public comment, or other collaboration. A complete Federal record must have content, context, and



structure along with associated metadata (e.g., author, date of creation). The complete record must be maintained to ensure reliability and authenticity.

Agencies should take the following actions when establishing social media policies and procedures:

- Identify what constitutes a Federal record in social media platforms.
- Define ownership of content and responsibility for managing the records.
- Incorporate recordkeeping practices and requirements into terms of service.
- Communicate records policies so employees and the public understand how records will be managed.
- Monitor the ongoing use of social media platforms to determine if that use changes the value of the records.
- Monitor any changes to third-party terms of service on social media platforms that may affect the management of records.

Content on social media is likely a Federal record. Agencies must identify the official record and determine how it will be managed. Some social media records may be temporary; with a transitory, short, or long term retention. Some may even be permanent, such as a blog by an agency senior official.

Once social media content is identified as Federal records and associated with an approved records schedule, agencies must decide how to manage social media records. Temporary records whose retention is transitory or short-term may not need to be captured and can be maintained in the social media platform. Agencies should assess their business needs and evaluate risks associated with leaving these records in social media. Capture is important for temporary records with long-term retentions or for permanent records. These should be exported from the social media platform into an agency recordkeeping system.

Methods to capture social media include:

- Using web crawling or other software to create local versions of sites.
- Using web capture tools to capture social media.
- Using platform-specific application programming interfaces (APIs) to pull content.
- Using RSS Feeds, aggregators, or manual methods to capture content.
- Using tools built into some social media platforms to export content.

The options for successful social media capture will depend on the technical configuration of a social media platform. Agency needs may also affect which social media capture method is used. Once the agency determines the capture method, they must provide training to applicable staff on how and when to use capture tools for social media. Agencies may need to work with third-party providers to implement social media capture.

Each agency is responsible for managing its records. At a minimum, these responsibilities include the ability to identify and retrieve Federal records that are being created and maintained on social media. Agencies should be aware that a social media provider could discontinue their service or delete information from an agency's account. Additionally, agencies may stop



using a social media platform at any time. In either situation, the agency is not relieved of its records management and possible capture obligations.

- For a deeper dive on any of the above visit: Bulletin 2014-02 | National Archives.
- Agency social media managers, content creators, and other staff should contact their agency records officers and office of general counsel to discuss social media records management issues. A list of agency records officers can be found on the NARA web site at <http://www.archives.gov/records-mgmt/agency/officers-lists.html>

Endorsements

Official/personal-professional Navy pages cannot appear to endorse another page, influencer or entity. What does this mean? DoD pages CANNOT outwardly post a call-to-action to follow any non-DoD pages; promote/attempt to sell products or raise funds for any for-profit or non-profit entity. Navy pages CAN “like” posts and/or follow pages that align with the Navy brand, reply to @ messages that tag them (if the page aligns with the Navy brand).

What does “align with Navy brand” mean? It means organizations or individuals who generally adhere to the same standards of moral conduct/professionalism. When scanning their pages, they do not/have not posted incendiary/racist/homophobic etc. content.

Please use caution and when in doubt consult your JAG should a question of potential endorsement arise.

Disclaimers should be added to all page bios that includes language “Following/Liking/Sharing ≠ (does not equal) endorsement.” DoD personnel may not use their official position for any financial gain or to promote any product, service or political campaign. Service members may NOT endorse any product, service, or political campaign while in uniform. Please refer to DoD Instruction 5400.17, Section 8, Appendix L in this playbook, for details.

Impersonators

In the fourth quarter of 2020, there were about 2.8 billion monthly active users on Facebook, according to their earnings report and Facebook estimates that **fake accounts represented 5% of monthly active users** in that same timeframe. (Source: Facebook Banned 1.3 Billion Accounts Over Three Months To Combat ‘Fake’ And ‘Harmful’ Content (forbes.com))

5% doesn’t sound like a lot, however, with the volume of active users on Facebook, that’s roughly **140 million accounts**.

What does this mean for Navy? This means that impersonations of officials are extremely likely. How do you protect against them? One way is to get your page verified. In order to do so, the following criteria is required:

For Facebook and Instagram, required info is as follows:

- PAGE URL:
- EMAIL:
- PROFILE URL:
- INSTAGRAM:



For Twitter: Only the Name of the page and @handle are required, however, the following criteria must also be met:

For all of the @handles you list you must add an email address to the account under “Account Information” at: https://twitter.com/settings/your_twitter_data/account. (While a government email address is preferred; it is not required. A confirmation email that will be sent to the email inbox of that address. Please tap the button to confirm.)

And pages must meet ALL of the following criteria:

- A profile photo that is not Twitter’s default photo.
- A header image that is not Twitter’s default photo.
- A link to a website with a .gov domain.
- A bio specific the person’s official title or purpose.
- Profile must be set as public, not private.

DOD PERSONNEL AND POLITICAL ACTIVITY: THE HATCH ACT

DoD Personnel and Political Activity: The Hatch Act

The U.S. Office of Special Counsel (OSC) routinely receives questions from federal employees and others about when the use of social media could violate the Hatch Act. Social media platforms are easily accessible to most employees while at work — on computers, smartphones, or other devices. OSC has created this guidance to help federal employees understand what the Hatch Act does and does not.

In general, all federal employees may use social media and comply with the Hatch Act if they remember the following three prohibitions:

1. On Duty or in the Workplace Prohibition — Employees may not engage in political activity while on duty or in the federal workplace.
2. 24/7 Prohibition — Employees may not knowingly solicit, accept, or receive a political contribution for a political party, candidate in a partisan race, or partisan political group.
3. 24/7 Prohibition — Employees may not use their official authority or influence to affect the outcome of an election.

Military Personnel: DoD has a longstanding policy of encouraging military personnel to carry out the obligations of citizenship. However, AD members will not engage in partisan political activities and all military personnel will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval or endorsement of a political candidate, campaign or cause.

Civilian Personnel: For DoD civilians, participation in political activity is regulated by a number of sources: the Hatch Act (5 U.S.C. §§ 7321 - 7326), implementing regulations (5 C.F.R. § 733 and 5 C.F.R. § 734), as well as DoD policy. For purposes of the Hatch Act, political activity is defined as “an activity directed toward the success or failure of a political party, candidate for partisan political office or partisan political group”. Because application of the rules may vary depending on an employee’s position or office, it is extremely important that employees who



are considering engaging in political activity know which rules apply.

With regard to civilian employees, there are two sets of restrictions for three groups of employees. The first and more restrictive set of restrictions applies to: (1) individuals appointed by the President and confirmed by the Senate and individuals serving in non-career SES positions; and (2) career members of the SES, contract appeals board members, and all employees of the National Security Agency (NSA), the Defense Intelligence Agency (DIA), and the National Geo-Spatial-Intelligence Agency (NGA). The second and more lenient set of restrictions applies to all other employees (including Schedule C political appointees).

Employees in Groups 1 and 2 are prohibited from taking an active part in partisan political management or political campaigns and are referred to as "further restricted" employees.

For further details on the above please see Appendix K.

RESOURCES

Fleet Resource Page.

GPA: Government, Politics and Advocacy Support Portal.

This team supports a range of technical, operational, and finance-related requests across Facebook and Instagram, including:

- ☒ Verified badge requests
- ☒ Disapproved ad appeals
- ☒ Name or username changes
- ☒ Fake account reports
- ☒ Duplicate account merges
- ☒ Hacked account reports
- ☒ Product questions or issues

Registering for GPA: In order to register for GPA and get verified on Facebook and Twitter, the following information is required of your team:

FB PAGE URL: <https://www.facebook.com/yourorganizationhandle>

EMAIL: john.doe_pao.mil@us.navy.mil

PROFILE URL: https://www.facebook.com/john.doe_pao

INSTAGRAM URL: <https://www.instagram.com/yourorganizationhandle>

TWITTER PAGE HANDLE: @yourorganizationhandle

*Please ensure your organization page bios are filled out **completely** on each platform with a link to your organization's respective website and/or navy.mil URL, then contact CHINFO for registration and assistance at **NavySM@us.navy.mil***

Once registered you can access GPA by visiting: <https://www.facebook.com/gpa>



For help on a variety of issues from requesting page verification to your account being hacked, visit: <https://www.facebook.com/gpa/help>

Don't forget to bookmark the above links so you can easily reach out for help whenever needed! Be sure you are logged into your Facebook account to access support and include your government or organization email address when submitting a request.

Reporting Impersonation Accounts

If you see a page that is in the likeness and name of your leadership or organization, is not verified, and is posting content that seems in misalignment with Navy values, or is selling, or attempting to solicit funds from people:

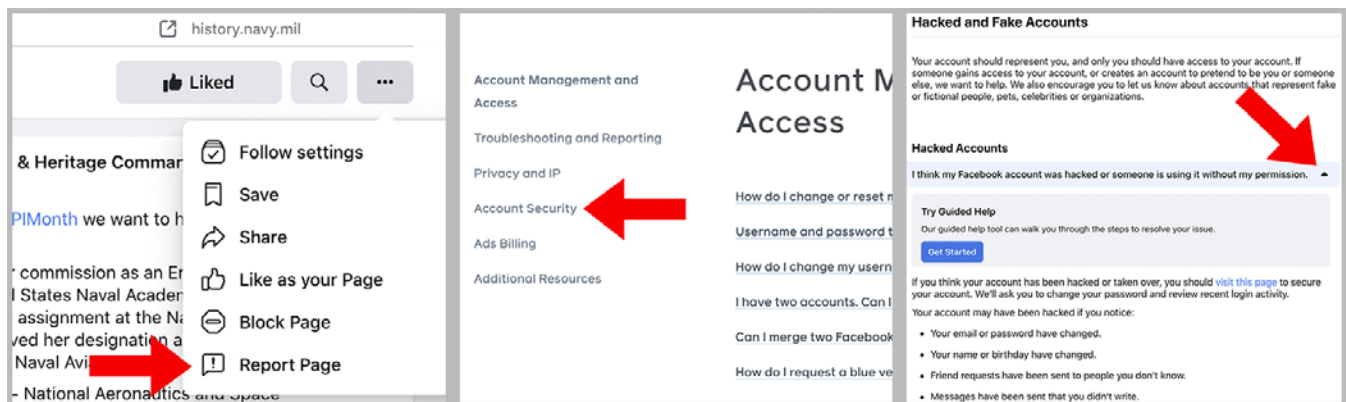
1. IMMEDIATELY REPORT THE PAGE WITHIN THE PLATFORM.
2. Report it to NCIS.
3. Once reported to platform and NCIS, please send an email NavySM@us.navy.mil with the following information:
 - URL of fake page.
 - URL of verified/official page.
 - Case number from the platform when you reported it (for Twitter only).

Hacked Accounts

If you feel you have been hacked and lose access to your account:

For Facebook:

1. Go to www.facebook.com/gpa/help
 - Click on Account Security
 - Click "I think my account or Page was hacked." follow the prompts.



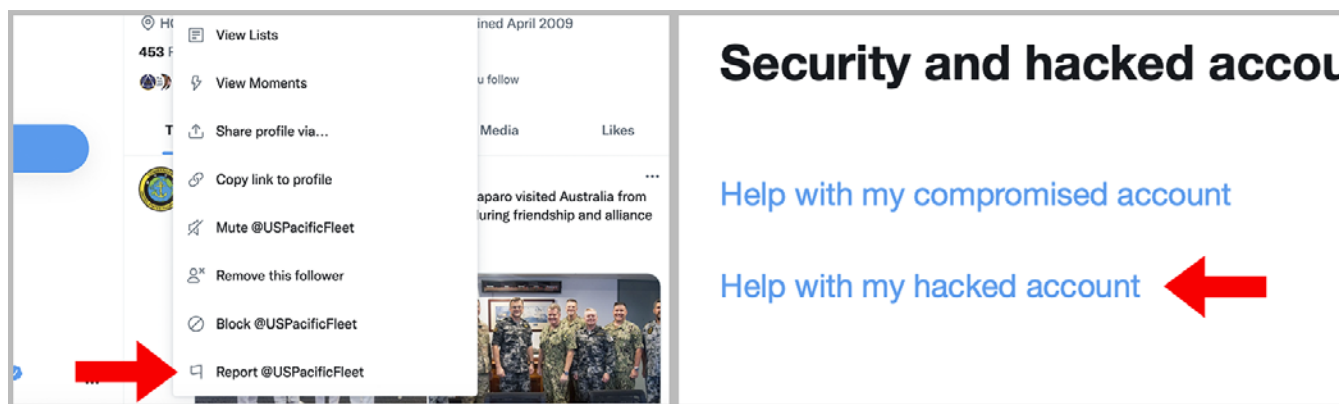
2. Report it to NCIS.
3. Send an email to NavySM@us.navy.mil with:
 - URL to your page.



- When you noticed the hacking and any actions taken not by you on the account.

For Twitter:

1. Go to <https://help.twitter.com/en/safety-and-security>; select compromised or hacked account and follow the prompts from there.
2. Report it to NCIS
3. Send an email to NavySM@us.navy.mil with:
 - URL to your page
 - Twitter case number



Reviving or Deleting Dead Accounts

What is a dead account? One that hasn't been posted to in the past quarter.

To remove the page altogether, send an email to NavySM@us.navy.mil with the page URL and the action you want taken. If you want to reclaim the page, send an email to NavySM@us.navy.mil with the page URL, the email addresses of the desired admins (for Facebook only) and the link to your command webpage.

HOW TO'S

Facebook

Steps to Create an Account:

1. A personal Facebook account is required in order to create a Facebook Page.
2. Login to your personal Facebook account, then go to <https://www.facebook.com/pages/create>
3. Choose the type of page you would like to create:
 - Local business or place
 - Artist, band, or public figure



- Company, organization, or institution
 - Entertainment
 - Brand or product
 - Cause or community
4. Enter in your company's info, review Facebook's terms, and click on "Get Started".
 5. Facebook will provide four tabs:
 - About
 - Profile Picture
 - Add to Favorite
 - Reach More People.
 6. Complete the fields within each tab and click on "Save Info".

Other Related Resources: Visit www.navy.mil/socialmedia

Instagram

Steps to Create an Account:

1. Download the Instagram app for Apple iOS from the App Store, Android from Google Play Store or Windows Phone from the Windows Phone Store.
2. Once the app is installed, tap to open it.
3. Tap "Register with Email" to sign up with your email address or "Register with Facebook" to sign up with your Facebook account.
4. If you register with email, create a username and password, fill out your profile info and then tap "Done".
5. If you register with Facebook, you'll be prompted to sign into your Facebook account if you're currently logged out.

Other Related Resources: Visit www.navy.mil/socialmedia

LinkedIn (company page)

Steps to Create an Account:

1. A personal LinkedIn account is required in order to create a LinkedIn Company Page.
2. Login to your personal LinkedIn account at linkedin.com.
3. Click on "Interests" > "Companies" > "Create" (in right column, under "Create a Company Page").



4. Enter in your company's name and your email address, and click on the check box to verify you are the official representative of the company.
5. To publish your company page, you must include a company description and company website URL.

Other Related Resources: Visit www.navy.mil/socialmedia

Twitter

Steps to Create an Account:

1. Go to twitter.com
2. Enter your full name, email address, and a password in the "New to Twitter? Sign up" box.
3. Click "Sign up for Twitter".
4. On the next page, you can select a username (usernames are unique identifiers on Twitter) – type your own or choose one Twitter suggest. Twitter will tell you if the username you want is available.
5. Double-check your name, email address, password, and username.
6. Click "Create my account".
7. You may be asked to complete a Captcha.
8. Twitter will send a confirmation email to the address you entered on sign up, click the link in that email to confirm your email address and account.

Other Related Resources: Visit www.navy.mil/socialmedia

YouTube

Steps to Create an Account:

1. A personal Google account is required to set-up a YouTube account.
2. Go to youtube.com/channel_switcher and login using your Google account username and password.
3. Click on "Create a new channel".
4. Fill out the details to create your new channel.
5. From here you can begin setting-up your profile and uploading videos to share.

Other Related Resources: Visit www.navy.mil/socialmedia





Steps to Create an Account:

1. Go to pinterest.com/business/create (if you have a personal account, make sure to log out).
2. Enter your email address & create a new password.
3. Fill out the details about your business and contact info for the person who will manage the account.
4. Review and accept the terms of service.
5. Click on "Create Account".

Other Related Resources: Visit www.navy.mil/socialmedia

POSTING TO FACEBOOK AND INSTAGRAM

How to schedule posts and stories

You can create and schedule posts and stories on Facebook Business Suite desktop:

This can help you save time and stay organized by scheduling ahead.

Before you begin

The steps below only apply if you're trying to schedule posts for Business Suite desktop. There is also a Business Suite mobile app. Before you start make sure:

1. You're working in the correct account. To select a different Facebook Page and Instagram account in Business Suite, click the dropdown menu in the top left of your sidebar.
2. Select the Facebook Page and Instagram account you want to create and schedule posts for.

Create and schedule stories

Go to Posts & Stories or Calendar to begin:

1. Click Create Story.
2. Select where you want to create or schedule a post for your Facebook News Feed, Instagram Feed, or both.
3. Click Upload Media and add a photo or video to your story.
4. Customize your story by cropping your media, or by adding text or stickers.
5. Preview how your story will look on Facebook and Instagram on the right.
6. Click Publish Story to publish immediately, or click the arrow to select Schedule Story to publish it later.

You can see your story in the Calendar on the date that it was scheduled or published.



Create and schedule posts

1. Go to Posts & Stories or Calendar to begin.
2. Click Create Post. You can also click Create Post from the Home.
3. Select where you want to schedule a post: Facebook News Feed, Instagram Feed, or both.
Note: If this is your first time to schedule a post, you may have to reconnect your Instagram account. Learn more about how to connect your Instagram account on Business Suite desktop.
4. Enter in all of the details of your post, including text, media and an optional link and location. Note: You can't add both a photo and link preview for Facebook posts. Links for Instagram posts won't load photo preview.
5. For Facebook News Feed-only posts, select whether you want to add a Call to Action to your post. This will add a button to your post and help encourage people to message you from your post.
6. For Facebook News Feed-only posts, select an optional Feeling/Activity to add to your post. Remember, you can only add either Call to Action or a Feeling/Activity to your post.
7. Preview your post on the right. To see a different preview, click on the dropdown on the top of the window or on the arrows on the top right. You can see how it will look on Facebook compared to Instagram or on desktop compared to phone.
8. Click Publish.
9. (Optional) To publish the post later, click the arrow next to Publish.
 - Then, click Schedule Post. Add the date and time you want to publish your post.
 - Click Schedule on the bottom right when you're ready to schedule your post.

Steps to create an Instagram Reel

1. Find Reels in the Instagram camera. Reels is located at the bottom of the Instagram camera.
2. Choose the length and creative tools. Select the length of your reel - 15 or 30 seconds, and pick from a variety of tools like Effects, Timer, Speed, and Align to make your reel more creative.
3. Record your reel. Record by tapping on the multi-clip shutter. Tap the multi-clip shutter again to stop recording. Reels can be recorded in a series of clips, all at once, or you can upload videos from your gallery. After recording, you can go back and trim or delete any previous clips in your video.
4. Publish your reel. Choose your cover image, add a caption, hashtags, or tag other accounts. If you have a public account, your reel has the chance to be seen and discovered by the wider Instagram community.

Reels audio and fair use

Can you use copyrighted audio when using Instagram Reels? YES.

But keep in mind: Depending on the type of account you have: Business, Creator etc. Instagram



gives you access to a music/audio library which you are free to use. The size of the libraries vary depending on account type. For example, “business” accounts are generally attempting to sell something and thus have smaller music libraries. “Creator” accounts, conversely, have broader access to music and audio. As official government accounts we can also make our accounts “creator” accounts as we are not in the business of selling products.

As long as you are using what you have access to in the library, based on your account type, you are covered. Once you post, you will see the title of the song or audio in the lower left corner along with the artist/creator. One area in which you should exercise caution is the use of music labeled as “original audio.” These tracks may be protected from free use by Reels creators and are best to avoid – even if they are trending. If there is audio in this category you really want to use, please consult your legal office who may provide guidance on a case-by-case basis.

Rule of Thumb: When in doubt, use what is available to you in the Instagram music library.

How to build a following

No matter the platform, despite the algorithms there are a few things that will lead to a consistently growing platform.

- **CONSISTENCY.** How many times can you post per day? Maintain that battle rhythm over time and watch your audience grow.
- **ENGAGING CONTENT.** Keep videos short and to the point. Choose visuals that would make you stop in your tracks (or on your feed).
- **AUTHENTICITY.** Keep your voice and what you post true to your “brand” and authentic. In the case of the Navy, our Sailors are our proof points. They tell the story like no one else can. Highlight and feature them. And when you notice Sailors who have grown their own followings, engage them about telling their Navy story on your platforms while enabling them to continue being themselves on their own.

ON THE HORIZON

This section is dedicated to up and coming platforms showing high rates of growth and adoption that we may not have entered yet, but are keeping an eye on. Please note: New and emerging platforms are covered under DoDI 5400.17. If you wish to jump in on a new platform, there is a process for vetting per section 4.2. under Defense Information Systems Agency; new platforms must be approved prior to engaging on a platform for official use.

TikTok

While use of TikTok is not banned at this time; TikTok is banned on government devices. While TikTok is widely used and growing in the U.S., we are asked to keep in mind that it is owned by China and that the full extent of data collection from the app is not clear.

- TikTok allows users to watch, create, and share 15-second videos shot on cellphones.
- The app was launched in 2016 by the Chinese technology company ByteDance.
- Now available in more than 150 different markets, TikTok has offices in Beijing, Los Angeles, Moscow, Mumbai, Seoul, and Tokyo.



- The app had about 1.1 billion active global users by early 2021 and is growing at a rapid pace especially among 18-24 year olds.

Twitch

- Twitch is an online platform/app used to watch and stream digital video broadcasts. Originally, it was focused almost entirely on video games, but has since expanded to include streams dedicated to artwork creation, music, talk shows, and the occasional TV series.
- The streaming service boasts over 2 million unique streamers every month and more than 17 thousand of these users earn money through the Twitch Partner program, a service that provides streamers with added features such as paid subscriptions and ad placements.
- Amazon purchased Twitch in 2014 and it remains one of the highest sources of internet traffic in North America.

Clubhouse

- Clubhouse is an audio-only social media app known for its unconstrained conversations, celebrity backers and invite-only status.
- Likened to something between call-in radio and a professional conference; or an interactive podcast. Users self-select into rooms based on interest, and engage in live conversation.
- The app is still in beta testing, but nonetheless reached 8 million downloads by mid-February 2021 despite enrollment on an invite-only basis.
- Elon Musk, Oprah Winfrey and Bill Gates have all appeared on the app.
- Clubhouse seemingly gives access to public figures and thought leaders in a more personal way than social media platforms.
- Content is generally non-recordable, so a major draw is catching a live session before it's gone.



NAVY SOCIAL MEDIA FO'C'SLE:

If you are a Navy Communications professional you are invited to Join our private Facebook group to stay engaged with the Navy social media community and share ideas and perspectives.

This is a creative space to collaborate and facilitate discussions among the community from content planning, to developing strategic campaigns, to simply discussing current social trends and inspiring creativity. Admins facilitate discussion questions, monitor activity, admit/remove users as appropriate.

If you are interested in this level of discussion and/or would like to become an admin for this group, please email **NavySM@us.navy.mil** in order to be added to the Facebook Group.



GLOSSARY

Avatar: A static or moving image or other graphic representation that acts as a proxy for a person or is associated with a specific digital account or identity, as on the internet: Not the blue animated characters, an avatar is another word for profile picture or icon that visually represents and identifies your organization on the social media platform.

Bio: Biography, or short description in profile that easily describes who and what your organization is about. Recommend sharing website links, common hashtags, contact information, or disclaimers in this section.

Bots: A software program that can execute commands, reply to messages, or perform routine tasks, as online searches, either automatically or with minimal human intervention (often used in combination): *a social media bot retweeting certain posts; a customer service chatbot to answer product questions*. Especially prevalent on Twitter, a bot is an automated account run by software capable of posting content or interacting with other users. Some bots pretend to be humans.

Catfishing: When a person assumes a false identity or personality on the internet, especially on social media websites, as to deceive, manipulate, or swindle.

Command Presence: A profile on a social networking website which is considered distinct from an actual user personal or personal-professional profile in that it is created and managed by at least one other registered user, usually Public Affairs staff or Mass Communication Specialist as a representation of a non-personal online identity for that command. These pages are listed by command and/or ship name vice and individual and push out content to tell the story of that particular command/ship and its mission writ large.

Content: Something that is to be expressed through some medium, as speech, writing, or any of the various arts.

Cover Photo: A header image on Facebook, Twitter, and YouTube that tells people what your organization is about at first glance upon coming to your page.

Disinformation: False information created intentionally and spread with the intent to deceive.

DM: Direct message, or not publicly posted communication between two accounts. Keep in mind, however, that this correspondence is only private to the extent that one user can screenshot and publish the conversation.

Engagements: Social media engagement measures the public shares, likes and comments for an online business' social media efforts. Engagement has historically been a common metric for evaluating social media performance. How people react to the content, including likes, comments, retweets, shares, reactions, and more.

Ephemeral Content: Sometimes called “disappearing content,” these social media posts delete automatically after a set amount of time has lapsed. Instagram and Snapchat stories disappear after 24 hours. However, content is also susceptible to screen recording or other methods of indefinitely capturing the content.



Feed: A social media feed is an updated list of all the new content posted by the user follows on social media platforms. This stream of content published by other users, most often the “homepage” and most common way to see and engage with posts. Rather than being purely chronological, most social media feeds are controlled by an algorithm.

Hashtag: A word or phrase preceded by a hash sign (#), used on social media websites and applications, especially Twitter, to identify digital content on a specific topic.

Header: Your header photo is the **image that spans the top of your Twitter, Facebook, or YouTube profile page**. It’s quite a bit larger than your profile photo so make sure to save it at the highest resolution possible. Because you have more room to be creative with this picture and it will likely be the first thing your visitors see, make it something captivating.

Identity Management: IdM and IAM are terms often used interchangeably, however identity management is more focused on a user identity (or username), and the roles, permissions, and groups that user belongs to. IdM also focuses on protecting identities through a variety of technologies such as passwords, biometrics, multi-factor authentication, and other digital identities.

Impressions: How many people potentially saw the post; how many times the post was shown in users’ feeds, can be duplicated, and different social media networks define (and therefore calculate) this metric a little differently.

Influencer: **One who exerts influence:** a person who inspires or guides the actions of others; often, specifically: a person who is able to generate interest in something (such as a consumer product) by posting about it on social media.

Internet Sites: Any website or web page.

Malinformation: Information that is known to be true but is intentionally distorted and spread to do harm.

Mentions: **Social mentions include any mention of your organization or personal brand on social media.** It’s important to remember this doesn’t only include the mentions that tag your page. There are tons of conversations about your organization on social media that you aren’t receiving notifications for. Keeping an eye on mentions, following what your audience is saying; more passive approach than social listening.

Microinfluencer: A micro-influencer is someone who has between **1,000 to 100,000 followers**. Micro-influencers focus on a specific niche or area and are generally regarded as an industry expert or topic specialist. “ [Micro-influencers] have stronger relationships than a typical influencer.

Misinformation: False information spread unintentionally.

Personal Page: Personal web pages are world wide web pages created by an individual to contain content of a personal nature rather than content pertaining to a company, organization or institution.

Personal-Professional Page: A page where you (or your team) represent(s) yourself as yourself; but in a professional capacity; tied to your official Navy title and in your official Navy capacity.

Platform: Also may be referred to as a social media “network” or social media “channel”.



Post: A post is a message, such as text or photos, published online by a user while referring to a message board, comment section, or social network.

Reach: **Post reach** is the number of people who saw a specific post in their news feed. **Page reach** is the number of people who saw any of your post content during a given period of time (daily, weekly or monthly).

Reels: **Reels** was created as a new way for users to create and discover short, entertaining videos on the platform. Unlike other short-form video platforms, **Reels** are 15 or 30-second multi-clip videos that you can record and edit them with audio, effects, and creative tools in a similar way to TikTok.

Social Listening: Tracking conversations around key topics and terms related to your brand, gathering mentions, comments, hashtags, and posts to provide insight on conversations surrounding your brand.

Social Monitoring: In basic terms, social media monitoring is the act of using a tool to listen to what is being said across the internet; monitoring media not just from traditional publishers, but on millions of social sites too.

Stories: See *Ephemeral Content*.

Target Audience: A particular group at which a film, book, advertising campaign, etc., is aimed.



APPENDIX A: ACCEPTABLE USE POLICY

U.S. NAVY ACCEPTABLE USE POLICY REQUIREMENTS APPLICABLE TO DON OFFICIAL SOCIAL MEDIA PRESENCES

REQUIREMENTS APPLICABLE TO DON OFFICIAL SOCIAL MEDIA PRESENCES.

1. **Administrators.** Commands and activities shall designate administrators for official social media properties in writing. The administrator is responsible for ensuring all posts and content comply with DOD, DON, and command policy. Commands permitting postings by others (i.e. takeovers) on their platforms must ensure those designated to do so are media trained and understand what is acceptable and not acceptable.
2. **Local Procedures.** Commands and activities must develop written local procedures to ensure the approval and release of all information posted on official social media platforms is in alignment with U.S. Navy guidance. SECNAVINST 5720.44C U.S. Navy Public Affairs Regulations (<https://dvidshub.net/r/3c4ayp>)
3. **Security.** Commands will actively monitor and evaluate official use of social media platforms for compliance with security requirements and for fraudulent or unacceptable use. Misuse of Navy brands or properties by imposters should be reported through the chain of command and/or to the Navy Office of Information (CHINFO) who can provide assistance and guidance as needed. Passwords to official pages as well as admin accounts supporting those pages must be changed at least quarterly and adhere to NMCI/DISA security protocols for strong passwords including upper, lowercase, numeric and special characters.
4. **Primary Web Presence.** A command or activity social media presence, including those on blog platforms, may not serve as a command's primary web presence, and must link to the command's official website.
5. **Prohibited Content.** Commands and activities shall not publish and shall prohibit content listed in the PA Regs CHAPTER 7 – PUBLIC COMMUNICATION ON THE INTERNET, Section 0702 REQUIREMENTS APPLICABLE ONLY TO DON WEBSITES, as well as:
 - a. Personal attacks, vulgar, hateful, violent, or racist language, slurs, stereotyping, hate speech, and other forms of discrimination based on any race, color, religion, national origin, disability, or sexual orientation.
 - b. Information that may elicit threats to the security of Navy and Marine Corps operations or assets, or to the safety of DON personnel and their families.
6. **Correcting the Record.** When engaging in the comments section on an official social media presence with those who have posted inaccurate or misleading information, remember to be respectful, clear, and concise providing factual, relevant information. Corrections to original posts on Navy platforms must acknowledge the issue (typo etc.) and be followed with a corrected post.
7. **Personal Posts to Blogs and Social Media Sites.** Individual members of the DON are authorized to participate in or operate blogs or other social networking services. The DON recognizes the value of these communication channels in posting current information and supporting the morale of personnel, their families, and friends. As long as personnel adhere



to operational security requirements regarding the public release of information, the DON encourages the use of blogs and social networking services. Furthermore, SECNAVINST 5720.44C CH-2 10 APR 2019 (Page 7-19) recognizes this free flow of information contributes to legitimate transparency of the DON to the American public. HOWEVER, any individual member of the DON who is identified as such, both directly or indirectly, on a blog or other social media service, may be perceived to represent the DON and must act accordingly. In addition to the types of information outlined in Chapter 7 of the PA Regs, the following information must not be displayed on personal pages operated by individual members:

- a. Any image, still or motion, of any military operation or activity (unless that image has been cleared for public release by the proper authority) if there is a potential for a security or privacy violation.
- b. Language that may tend to diminish the confidence in or respect for his or her superior(s), per the Uniform Code of Military Justice.



APPENDIX B: REQUIRED DISCLAIMER

COMMUNITY GUIDELINES:

Welcome to the [Your Command/Organization] Facebook page. For the latest Navy news, please visit our official website at <http://www.navy.mil>. While this is an open forum, it's also a family friendly one, so please keep your comments and wall posts CLEAN and free from profanity.

NOTE: Comments and posts that do not adhere to the following guidelines will be removed or hidden. Continual violation of these guidelines will result in being blocked from this platform:

- We do not allow graphic, obscene, explicit or racist comments or submissions, nor do we allow comments that are abusive, hateful or intended to defame anyone or any organization.
- We do not allow solicitations or advertisements. This includes promotion or endorsement of any financial, commercial or non-governmental agency. Similarly, we do not allow attempts to defame or defraud any financial, commercial or non-governmental agency.
- We do not allow comments that suggest or encourage illegal activity.
- Apparent spam will be removed and may cause the author(s) to be blocked from page without notice.
- You participate at your own risk, taking personal responsibility for your comments, your username and any information provided.
- For Official Use Only (FOUO), classified, pre-decisional, proprietary or business sensitive information should never be discussed here. Don't post personnel lists, rosters, organization charts or directories.
- Service members and their families/friends: Please practice good operations security (OPSEC); never share personal information, mission/deployment schedules or any other personally identifiable information (PII) or on any other publicly available information here (PAI). This includes all government websites and social media platforms.
- The appearance of external links on our Facebook page does not constitute official endorsement on behalf of the U.S. Navy or Department of Defense.
- You are encouraged to quote, republish or share any content on this page on your own blog, website or other communication/publications.

Thank you for your interest in and support of the U.S. Navy!



APPENDIX C: REFERENCES

Code of Federal Regulations, Title 5, Section 2635

DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 30 1993, as amended

Administrative Instruction 15, "OSD Records and Information Management Program," May 3, 2013, as amended

DoD Directive 1344.10, "Political Activities by Members of the Armed Forces," February 19, 2008

DoD Directive 3115.18, "DoD Access to and Use of Publicly Available Information (PAI)," June 11, 2019, as amended

DoD Directive 5122.05, "Assistant to The Secretary of Defense for Public Affairs (ATSD(PA))," August 7, 2017

DoD Directive 5535.09, "DoD Branding and Trademark Licensing Program," December 19, 2007

DoD Instruction 1304.35, "Military Marketing," November 1, 2017, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019

National Archives Records Administration Bulletin 2014-02, "Guidance on managing social media records," October 25, 2013

Office of Government Ethics' (OGE) Legal Advisory, LA-14-08, "Reference to Official Title and Position by Employees Affiliated with Outside Organizations in Their Personal Capacity," November 19, 2014

Office of Government Ethics' Legal Advisory, LA-15-03, "The Standards of Conduct as Applied to Personal Social Media Use," April 9, 2015

United States Code, Title 5, Section 7321-7326

United States Code, Title 15, Section 6501-6505

United States Code, Title 44, Section 2911

Harassment Prevention and Response in the Armed Forces (DoDI 1020.03)

Information Collection under the Paperwork Reduction Act (PRA) (OMB Memo)

Joint Ethics Regulation (DoD 5500.7-R)

Management of The Department of Defense Information Enterprise (DoDD 8000.01)

Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (OMB Memo)


Standards of Conduct (DoDD 5500.07)


DoD Vulnerability Disclosure Policy

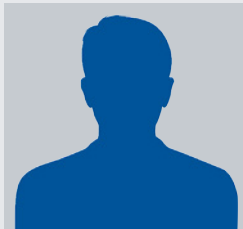
DODI 5400.13 Public Affairs (PA) Operations



APPENDIX D: USER PERSONA TEMPLATES

	Age/Generation	Media Activity Facebook <input type="text"/> Instagram <input type="text"/> Twitter <input type="text"/> Snapchat <input type="text"/> YouTube <input type="text"/> Cable TV <input type="text"/> Newspaper & Print <input type="text"/>
	Occupation	
	Location	
	Archetype	
Goals		

	Age/Generation	Media Activity Facebook <input type="text"/> Instagram <input type="text"/> Twitter <input type="text"/> Snapchat <input type="text"/> YouTube <input type="text"/> Cable TV <input type="text"/> Newspaper & Print <input type="text"/>
	Occupation	
	Location	
	Archetype	
Goals		

	Age/Generation	Media Activity Facebook <input type="text"/> Instagram <input type="text"/> Twitter <input type="text"/> Snapchat <input type="text"/> YouTube <input type="text"/> Cable TV <input type="text"/> Newspaper & Print <input type="text"/>
	Occupation	
	Location	
	Archetype	
Goals		



APPENDIX E: KEY CHANNELS TEMPLATE

	Demographic	Content	Voice	Where to Submit Content
Facebook				
Twitter				
Instagram				
Navy.mil				
YouTube				
Pinterest				
LinkedIn				
Snapchat				
Twitch				



APPENDIX F: CHANNEL OPTIMIZATION TEMPLATE

Platform	Frequency	Optimal Times



APPENDIX G: FORMAT SPECS PER PLATFORM

Each platform has its own format preferences in terms of file size and orientation

FACEBOOK

Product	Resolution	Aspect Ratio	File Size	File Format	Length	Frame Rate
Shared Post Video Landscape	1280 x 720	16:9	4 GB	.MP4 or .MOV (recommended)	240 minutes	30 fps
Shared Post Video Portrait	720 x 1280	9:16	4 GB	.MP4 or .MOV (recommended)	240 minutes	30 fps
360 Video	Monoscopic: 5120 x 2560 maximum Stereoscopic: 5120 x 5120 maximum	Monoscopic: 2:1 Stereoscopic: 1:1	10 GB	.MP4 or .MOV (recommended)	30 minutes	30 fps
Stories		1.91 to 9:16	4 GB	.MP4 or .MOV (recommended)	15 seconds	
Profile Photo	180 x 180	1:1		JPG, PNG		
Cover Photo	820 x 312	2.7:1				
Shared Image (Timeline)	1200 x 630	1.91:1				
Shared Image (Newsfeed)	1200 x 630	1.91:1				
Shared Link (Timeline)	1200 x 628	1.91:1				
Shared Link (Newsfeed)	1200 x 628	1.91:1				
Event Image	1920 x 1080	16:9				

INSTAGRAM

Product	Resolution	Aspect Ratio	File Size	File Format	Length	Bit Rate	Frame Rate
In Feed Landscape Video	1080 x 1080	16:9	4 GB	.MP4 or .MOV (recommended)	2 minutes	5 MBPS	23 - 60 fps
In Feed Square Video	1080 x 1080	1:1	4 GB	.MP4 or .MOV (recommended)	2 minutes	5 MBPS	23 - 60 fps
In Feed Vertical Video	1080 x 1080	4:5	4 GB	.MP4 or .MOV (recommended)	2 minutes	5 MBPS	23 - 60 fps



Product	Resolution	Aspect Ratio	File Size	File Format	Length	Bit Rate	Frame Rate
Instagram Stories (Organic)	1080 x 1920	9:16	4 GB	.MP4 or .MOV (recommended)	15 seconds	5 MBPS	23 - 60 fps
Instagram Reels	1080 x 1920	9:16	4 GB	.MP4 or .MOV (recommended)	15 seconds or 30 seconds		
IGTV	1080 x 1920	9:16 (recommended) or 16:9. In feed previews = 4:5	650 MB (under 10 minutes) or 3.6 GB (up to 60 minutes)	.MP4	15 minutes when uploaded from mobile (60 minutes on desktop)		
Profile Picture	110 x 110						
Photo Thumbnails	161 x 161						
Photo Size (Instagram App)	1080 x 1080 (square) 1080 x 1350 (4:5)	Between 1.91:1 and 4:5					
Instagram Stories	1080 x 1920	9:16					

TWITTER

Product	Resolution	Aspect Ratio	File Size	File Format	Length	Frame Rate
Landscape Video	1280x720 (landscape) 720x1280 (portrait) 720x720 (square)	16:9 (landscape or portrait) 1:1 (square)	512 MB	.MP4 or .MOV	140 seconds	30 or 60 fps
Portrait Video	1280x720 (landscape) 720x1280 (portrait) 720x720 (square)	16:9 (landscape or portrait) 1:1 (square)	512 MB	.MP4 or .MOV	140 seconds	30 or 60 fps
Profile Photo	400 x 400	1:1	2 MB			
Header Photo	1500 x 500	3:1	5 MB			
Image from a Tweet with shared link	1200 x 628 (recommended)	16:9 (recommended)	5 MB			
Tweet sharing a single image	1200 x 675 (recommended)	16:9 (recommended)	5 MB			
Tweet sharing two images	700 x 800 (per image)	16:9 (recommended)	5 MB			
Tweet sharing three images	Left image: 700 x 800 Right images: 1200 x 686	16:9 (recommended)	5 MB			
Tweet sharing four images	1200 x 600 (per image)	16:9 (recommended)	5 MB			



LINKEDIN

Product	Resolution	Aspect Ratio	File Size	File Format	Length	Frame Rate
Shared Video		1:2.4 to 2.4:1	5 GB	.ASF, .AVI, .FLV, .MOV, .MPEG-1, .MPEG-4, .MKV, .WebM, .MP4	10 minutes max	60 fps
Personal Profile Image	300 x 300		8 MB	PNG, JPG, GIF		
Personal Background Image	1584 x 396		4 MB	PNG, JPG, GIF		
Company Logo Image	300 x 300		4 MB	PNG, JPG, GIF		
Company Main Image	1128 x 191		4 MB	PNG, JPG, GIF		
Shared Link	1200 x 627			PNG, JPG, GIF		
Shared Image	1200 x 627			PNG, JPG, GIF		
Life Tab: Main Image	1128 x 376		2 MB	PNG, JPG, GIF		
Life Tab: Company Photos	900 x 600			PNG, JPG, GIF		

PINTEREST

Product	Resolution	Aspect Ratio	File Size	File Format	Length
Standard Video		1:1 (square) or 2:3, 4:5, or 9:16 (vertical)	2 GB	.MP4 or .MOV	4 seconds to 15 minutes
Max Width Video		1:1 (square) or 16:9 (widescreen)	2 MB	.MP4 or .MOV	4 seconds to 15 minutes
Profile Picture	165 x 165		10 MB	JPG, PNG	
Pins (Main Page)		2:3 - 1:3.5			
Pins (On Board)		2:3 - 1:3.5			
Pins (Expanded)	600 width, height scales 900 recommended height	2:3 - 1:3.5			
Pin Board (Large Thumbnail)	222 x 150				
Pin Board (Smaller Thumbnail)	55 x 55				



YOUTUBE

Product	Resolution	Aspect Ratio	File Size	File Format	Length
240p Video	426 x 240	16:9 (4:3 auto adds pillarboxing)	128 GB or 12 hours (whichever is less)	.MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, 3GPP, WebM	12 hours max
360p Video	640 x 360	16:9 (auto adds pillarboxing if set at 4:3)	128 GB or 12 hours (whichever is less)	.MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, 3GPP, WebM	12 hours max
480p Video	854 x 480	16:9 (auto adds pillarboxing if set at 4:3)	128 GB or 12 hours (whichever is less)	.MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, 3GPP, WebM	12 hours max
720p Video	1280 x 720	16:9 (auto adds pillarboxing if set at 4:3)	128 GB or 12 hours (whichever is less)	.MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, 3GPP, WebM	12 hours max
1080p Video	1920 x 1080	16:9 (auto adds pillarboxing if set at 4:3)	128 GB or 12 hours (whichever is less)	.MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, 3GPP, WebM	12 hours max
1440p Video	2560 x 1440	16:9 (auto adds pillarboxing if set at 4:3)	128 GB or 12 hours (whichever is less)	.MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, 3GPP, WebM	12 hours max
2160p Video	3840 x 2160	16:9 (auto adds pillarboxing if set at 4:3)	128 GB or 12 hours (whichever is less)	.MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, 3GPP, WebM	12 hours max
Channel Profile Image	800 x 800				
Channel Cover Art	2560 x 1440				
Channel Cover: Safe area for logos and text	1235 x 338				
Video Uploads	Minimum HD 1280 x 720	16:9			

SNAPCHAT

Product	Resolution	Aspect Ratio	File Size	File Format	Length
10-Second Video (Stories)	1080 x 1920	9:16	32 MB	.MP4 or .MOV	3 to 10 seconds

Source: <https://sproutsocial.com/insights/social-media-image-sizes-guide>



APPENDIX H: BLANK PLANNING CALENDAR

MONTH:	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday



APPENDIX I: CALENDAR DATES

January	February	March	April	May	June
<p>Theme: New Year and Navy Resilience</p> <ul style="list-style-type: none"> • 1 - New Year's Day • 15 - National Hat Day • Third Monday - Martin Luther King Jr. Day • 24 - National Compliment Day • 25 - National Spouses Day • 27 - Holocaust Remembrance Day • 28 - Space Shuttle Challenger Disaster • 28 - Data Privacy Day <p>Focus: Various aspects of toughness – mental, emotional, and physical to carry Sailors throughout the year.</p>	<p>Theme: Excellence in Service</p> <ul style="list-style-type: none"> • Black History Month • Super Bowl • 1 - Space Shuttle Columbia Disaster • 2 - Groundhog Day • 9 - National Pizza Day • 14 - Valentines Day • 19 Feb-Mar 26 - Battle of Iwo Jima • National Engineers Week • 20 - Love Your Pet Day • Third Monday - Presidents' Day • 22 - First Navy designated female aviator to earn her wings <p>Focus: Aspiring to greatness through service.</p>	<p>Theme: Women in Service</p> <ul style="list-style-type: none"> • Women's History Month • 2 - First four women pilots begin training in the U.S. Navy • 3 - Navy Reserve Birthday • 5 - Seabee Birthday • 6 - National Employee Appreciation Day • 8 - International Women's Day • 9 - Battle of Hampton Roads • 13 - K9 Veterans Day • 14 - National Pi Day • Second Sunday - Daylight Saving Time Begins • 17 - Saint Patrick's Day • 19 - National Let's Laugh Day • 20 - Spring Equinox • 21 - World Poetry Day • 22 - World Water Day • 25 - Medal of Honor Day • 29 - National Vietnam Veteran's Day • 30 - National Doctors' Day <p>Focus: Women's accomplishments in the U.S. Navy and their contributions to the fight.</p>	<p>Theme: Sailors are People, Too</p> <ul style="list-style-type: none"> • Mar or April - Easter • Month of the Military Child • Military Saves Month • 1 - Chief Petty Officer Birthday • 1 - April Fools Day • 5 - Gold Star Spouses Day • 10 - National Siblings Day • 11 - Submarine Birthday • 11 - National Pet Day • 16 - National High Five Day • National Volunteer Week • 22 - Earth Day • 27 - Holocaust Remembrance Day • 28 - Pay it Forward Day • 30 - Department of the Navy is established <p>Focus: Sharing personal Sailor stories, and what connects them to others without Navy ties.</p>	<p>Theme: Strength in Diversity</p> <ul style="list-style-type: none"> • NYC Fleet Week • Asian Pacific Heritage Month • Mental Health Awareness Month • 1 - National Explosive Ordnance Disposal Day • 4 - Beginning of the Battle of the Coral Sea • 4 - Star Wars Day • 6 - National Nurses Day • 8 - Birth of Naval Aviation • Friday before Mother's Day - Military Spouse Appreciation Day • Second Sunday - Mother's Day • 15 - International Day of Families • 13 - Nurse Corps Birthday • Third Saturday - Armed Forces Day • 22 - Maritime Day • Last Monday - Memorial Day <p>Focus: Sharing personal Sailor stories, and what connects them to others without Navy ties.</p>	<p>Theme: Where Old meets New</p> <ul style="list-style-type: none"> • 1 - National Say Something Nice Day • 4-7 - Battle of Midway • 6 - D-Day • 8 - Best Friends Day • 8 - U.S. Navy and USPS deliver the first official 'Missile Mail' • 12 - Women Veterans Day • 14 - Flag Day • 14 - Army Birthday • 19 - Juneteenth National Independence Day • 19 - Beginning of the Battle of Philippine Sea • Third Sunday - Father's Day • 21 - National Selfie Day • 30 - Social Media Day <p>Focus: Making Navy relevant to today's Gen Z and late millennial audiences. What are we doing that directly impacts their lives? Let's convey it!</p>



July	August	September	October	November	December
<p>Theme: All Navy Summer</p> <ul style="list-style-type: none"> • 1 - Samuel L. Gravelly Jr. becomes first African-American flag officer • 4 - Independence Day • 7 - World Chocolate Day • 15 - Give Something Away Day • 17 - World Emoji Day • 20 - Anniversary of the Moon Landing • 26 - President Truman desegregates the Military in 1948 • 30 - WAVES is established <p>Focus: Engaging Sailors and influencers in your command and AO to tell the Navy story in new and engaging ways.</p>	<p>Theme: Navy Worldwide</p> <ul style="list-style-type: none"> • 4 - Coast Guard Birthday • 7 - Purple Heart Day • 8 - International Cat Day • 9 - National Book Lovers Day • 15 - National Relaxation Day • 16 - National Tell a Joke Day • 19 - World Photo Day • 19 - National Aviation Day • 26 - National Dog Day • 30 - International Friendship Day <p>Focus: Navy Partnerships and exercises across the globe. Engage our partners in completing virtual PASSEXs where we all share content on the same day and tag each other in previous exercises.</p>	<p>Theme: My Shipmate's Keeper</p> <ul style="list-style-type: none"> • 15 Sep-15 Oct - Hispanic Heritage Month • Suicide Prevention Month • First Monday - Labor Day • 6 - Read a Book Day • 11 - Day of Service and Remembrance • First Sunday after Labor Day - National Grandparents Day • 17 - Constitution Day • 18 - Air Force Birthday • 21 - International Day of Peace • 22 - First Day of Fall <p>Focus: Encouraging Sailors to check on their Shipmates, engage in mental wellness activities and self-care, reiterate leadership support and caring.</p>	<p>Theme: Awareness. . . and Cake!</p> <ul style="list-style-type: none"> • Breast Cancer Awareness Month • Cyber Awareness Month • 1 - World Smile Day • 1 - National Coffee Day • Second Monday - Columbus Day • 13 - Navy Birthday • 13 - National Train Your Brain Day • 14 - National Dessert Day • 16 - Boss's Day • 21 - USS Constitution's Birthday • 27 - Navy Day • 30 - Checklist Day • 31 - Halloween <p>Focus: Keeping folks informed and aware about Breast Cancer and Cyber security facts and prevention; while celebrating Latinx Sailors, Navy Birthday/Day, Smiles and Halloween!</p>	<p>Theme: Thankfulness, Service and Sacrifice</p> <ul style="list-style-type: none"> • American Indian Heritage Month • Tuesday after the First Monday - Election Day • First Sunday - Daylight Saving Time Ends • 10 - Marine Corps Birthday • 11 - Veterans Day • 20 - National Entrepreneurs Day • Last Thursday - Thanksgiving Day • Last Friday - Black Friday • Last Saturday - Small Business Saturday • Monday after Thanksgiving - Cyber Monday • Tuesday after Thanksgiving - Giving Tuesday <p>Focus: Veteran appreciation and gratitude.</p>	<p>Theme: Giving Back through the Holidays</p> <ul style="list-style-type: none"> • Late Nov or Dec - Hanukkah • 4 - National Cookie Day • 7 - Pearl Harbor Remembrance Day • 10 - Human Rights Day • 21 - First Day of Winter • 25 - Christmas • 26 Dec-Jan 1 - Kwanzaa • 31 - New Year's Eve <p>Focus: Showcasing how Sailors give back to their communities and what they do for the holidays.</p>



APPENDIX J: NAVAL HISTORY DATES OF INTEREST

Dates in history with significant anniversaries in 2023.

Jan. 10, 1953	(70) The auxiliary motor minesweepers Merganser (AMS-26) and Firecrest (AMS-10) receive 40 rounds of 105 mm enemy fire from guns in the vicinity of Ponggang-ni near North Korea. Reports reflect no damage or casualties from the attack.
Jan. 12, 1953	(70) Aircraft begin operational landing tests, day and night, onboard USS Antietam (CVA-36), the first angled flight deck carrier.
Jan. 27, 1973	(50) The Paris Peace Accords are signed, ending U.S. participation in the Vietnam War.
Feb. 2, 1848	(175) The Treaty of Guadalupe Hidalgo ends the Mexican-American War and establishes the boundaries between the two republics.
Feb. 6, 1973	(50) In accordance with the agreement at the Paris Peace Talks, Navy Task Force 78 begins Operation End Sweep, the mine clearance of North Vietnamese waters of mines laid in 1972.
Feb. 8, 1953	(70) USS Lyman K. Swenson (DD-729) conducts counterbattery fire on a gun-shelling Korean sampans in the Kojo area, silencing the enemy guns.
Feb. 15, 1898	(125) The battleship Maine explodes in Havana Harbor, and nearly three-quarters of the battleship's crew die because of the blast. Popular opinion blames Spain, and the Spanish-American war starts soon after.
Feb. 20, 2018	(5) The crew of a Navy P8-A Poseidon belonging to the "Fighting Tigers" of Patrol Squadron (VP) 8 locate three missing fishermen in a 19-foot skiff from Chuuk Lagoon in the Federated States of Micronesia.
Feb. 23, 2018	(5) Independence-variant littoral combat ship, the future USS Omaha (LCS-12) is commissioned in a ceremony at the Broadway pier in San Diego.
Feb. 27, 1973	(50) First airborne mine sweep in a live minefield takes place in the Haiphong, Vietnam, ship channel by helicopters from Helicopter Mine Countermeasures Squadron Twelve on board USS New Orleans (LPH-11).
March 1, 1953	(70) During the Korean War, USS Valley Forge (CVA-45) aircraft raid the No. 1 power plant at Chosen, Korea, and heavily damage the strongly defended industrial site.
March 2, 1973	(50) The first four female U.S. Navy pilots begin training: Lt. j.g. Barbara A. Allen; Lt. j.g. Judith A. Neuffer; Ensign Jane M. Skiles; and Ensign Kathleen L. McNary.
March 5, 2018	(5) A detachment of F-35B Lightning II's with Fighter Attack Squadron 121 (VMFA-121) arrived aboard the amphibious assault ship USS Wasp



	(LHD-1), marking the first time the aircraft has deployed aboard a U.S. Navy ship and with a Marine expeditionary unit in the Indo-Pacific.
March 5, 2018	(5) USS Carl Vinson (CVN-70) arrives in Da Nang, Vietnam, for a scheduled port call, marking the first time a U.S. aircraft carrier has visited the country in more than 40 years.
March 7, 2018	(5) Commander, Submarine Forces (COMSUBFOR) officially kicks off Ice Exercise (ICEX) 2018 in the Arctic Ocean with the construction of temporary Ice Camp Skate and the arrival of two U.S. Navy fast-attack submarines and one U.K. Royal Navy submarine.
March 10, 1948	(75) The carrier suitability of the FJ-1 Fury jet fighter is tested aboard USS Boxer (CV-21) off San Diego, with a number of landings and takeoffs.
March 14, 2018	(5) Two U.S. naval aviators die when their F/A-18F Super Hornet crashes on final approach near Naval Air Station, Key West, Florida. Lt. Cmdr. James Brice Johnson and Lt. Caleb Nathaniel King were assigned to the "Blacklions" of Strike Fighter Squadron Two One Three (VFA-213), based at Naval Air Station Oceana and assigned to Carrier Air Wing Eight.
March 15, 1953	(70) Marine pilots of VMA 312 destroy eight rail cars, two possible radar towers, a power transformer and numerous other assorted targets in Korea before returning to USS Bataan (CVL-29).
March 17, 1898	(125) John Holland's submarine, Holland IV, performs the first successful diving and surfacing tests off Staten Island, NY.
March 17, 2018	(5) The 15th Virginia-class attack submarine, USS Colorado (SSN-788), is commissioned during a ceremony at Naval Submarine Base New London, CT.
March 23, 1953	(70) During the Korean War, jet aircraft from USS Oriskany (CVA-34) stage a "lights out" program by attacking a waterpower site below the Fusen Reservoir, resulting in four cuts in the intake structures that control the flow of water to the hydroelectric turbines and damaging two buildings housing generators.
March 23, 2018	(5) The guided-missile destroyer USS Ralph Johnson (DDG-114) is commissioned during ceremony at Columbus Street Pier in Charleston, SC.
March 25, 1898	(125) Assistant Secretary of the Navy Theodore Roosevelt recommends to Secretary of the Navy John D. Long that he appoint two officers "of scientific attainments and practical ability" who, with representatives from the War Department, would examine Professor Samuel P. Langley's flying machine and report upon its practicability and its potential for use in war.
March 27, 2018	(5) Guided-missile cruiser USS Hue City (CG-66) rescues three fishermen off the coast of Georgia.
March 28, 1848	(175) USS Supply, commanded by Lt. William F. Lynch, reaches the Bay of Acre, Israel, during an expedition to explore the Dead Sea and tracing the River Jordan to its source.



March 28, 1953	(70) USS Philippine Sea (CV-47), USS Princeton (CV-37), and USS Oriskany (CV-34) launch 216 sorties against a North Korean supply depot during the Korean War.
March 30, 1973	(50) USS Forrestal (CVA-59) and Sixth Fleet ships provide aid to Tunisia following a disastrous flood, relocating 729 persons, 27 tons of cargo, and an entire herd of 227 sheep.
April 4, 2018	(5) Medal of Honor Recipient Capt. Thomas J. Hudner Jr. is laid to rest at Arlington National Cemetery. Hudner was awarded the Medal of Honor for his actions in trying to save the life of his wingman during the Battle of Chosin Reservoir during the Korean War.
April 6, 2013	(10) The commissioning ceremony for USS Arlington (LPD-24) is held at Naval Station Norfolk, the ship's homeport. The San Antonio-class amphibious transport dock ship joins sister ships USS New York and Somerset in being named for the sites attacked by terrorists on Sept. 11, 2001. Steel salvaged from the Pentagon, based in Arlington, are showcased in the ship's museum.
April 8, 1823	(200) The barges USS Mosquito and USS Gallinipper, and sloop-of-war Peacock chase the pirate schooner, Pilot, which is driven ashore off Havana, Cuba.
April 8, 1848	(175) The first U.S. flag is flown over the Sea of Galilee when Lt. William F. Lynch sails in an iron boat up the Jordan River. He later authors a book, "Narrative of the United States' Expedition to the River Jordan and the Dead Sea."
April 9, 1848	(175) A party of men from the sloop-of-war USS Dale march 12 miles inland from Guaymas, Mexico, to capture and spike a 3-gun Mexican battery that was firing at other ships.
April 12, 2003	(20) USS Mason (DDG-87) is commissioned at Cape Canaveral, FL. The Arleigh Burke-class destroyer is the 37th in the class and the ninth of the Flight IIA variant.
April 12, 2018	(5) The F-35 program accomplishes the final developmental test flight of the system development and demonstration phase of the program.
April 13, 2018	(5) U.S., French, and British forces strike targets in Syria as punishment for Syrian leader Bashar Assad using chemical weapons against his own people.
April 14, 1898	(125) The first post-Civil War hospital ship, USS Solace (AH-2) is commissioned and soon participates in the Spanish-American War, attending to wounded servicemen from battles in Cuba.
April 18, 1848	(175) U.S. Navy expedition to explore the Dead Sea and the River Jordan, commanded by Lt. William F. Lynch, reaches the Dead Sea.
April 20, 1953	(70) USS New Jersey (BB-62) shells Wonsan, Korea, from inside the harbor during the Korean War.



April 21, 1898	(125) President William McKinley orders the Navy to begin a blockade of Cuba and Spain, the beginning of the Spanish-American War. Congress responds with a formal declaration of war April 25, made retroactive to the start of the blockade.
April 22, 1898	(125) Rear Adm. William T. Sampson leaves Key West, FL, with the North Atlantic Squadron to begin the blockade of the northern Cuban ports, the beginning of the Spanish-American War.
April 23, 1953	(70) After five UN personnel are wounded on island of Tee-do, Korea, USS Henderson (DD-785) is sent to suppress gunfire, and USS Owen (DD-536) evacuates the wounded to USS Manchester (CL-83).
April 24, 2018	(5) Amphibious transport dock USS Portland (LPD-27) is commissioned during a ceremony in her namesake city.
April 25, 1998	(25) The guided missile destroyer USS McFaul (DDG-74) is commissioned at Garden City Terminal in Savannah, GA. The 24th Arleigh Burke-class destroyer is named after Chief Petty Officer Donald L. McFaul, a Navy SEAL who posthumously received the Navy Cross for attempting to save a platoon mate on Dec. 20, 1989, while serving in Panama during Operation Just Cause.
April 25, 1998	(25) The first-in-class Impeccable (T AGOS-23) is launched from Pascagoula, MS. The ship is given to Military Sealift Command to be operated by civilian and military crewmembers.
April 26, 1923	(100) The General Board completes a study on U.S. Navy strategy in the Pacific that anticipates Japan as the only enemy in the foreseeable future. It calls for the development of bases at Pearl Harbor, Guam and in the Philippines and advocates for a fleet capable of sustained operations in the Western Pacific.
April 30, 1798	(225) Congress establishes the Department of the Navy as a separate cabinet department. Previously, naval matters were under the cognizance of the War Department. Benjamin Stoddert is named as the first Secretary of the Navy.
May 1, 1898	(125) The American squadron, commanded by Commodore George Dewey, defeats the Spanish squadron under the command of Rear Adm. Montojo at Manila Bay, Philippines.
May 4, 2013	(10) USS Anchorage (LPD-23) is commissioned in her namesake city. The San Antonio-class amphibious transport dock is the second ship to be named after the Alaskan city.
May 5, 1948	(75) Fighter Squadron Seventeen A (VF-17A), with 16 FH-1 Phantoms, becomes the first carrier-qualified jet squadron in the U.S. Navy.
May 11, 1898	(125) During the Spanish-American War, Marines and Sailors from USS Marblehead (C-11) and USS Nashville (PG-7) cut the transoceanic cable near Cienfuegos, Cuba, isolating Cuba from Spain. For heroism during this action, 54 Marines and Sailors received the Medal of Honor.



May 17, 1973	(50) Capt. Robin Lindsay Catherine Quigley becomes the first woman to hold a major Navy command when she assumes command of U.S. Navy Service School, San Diego, CA.
May 18, 1898	(125) During the Spanish-American War, boat parties from USS St. Louis and USS Wompatuck, under Capt. Caspar F. Goodrich, cut communication cables at Santiago, Cuba.
May 24, 2018	(5) President Donald J. Trump presents the Medal of Honor to retired Master Chief Special Warfare Operator (SEAL) Britt Slabinski during a ceremony at the White House in Washington, D.C. Slabinski received the Medal of Honor for his actions while leading a team under heavy effective enemy fire in an attempt to rescue teammate Petty Officer First Class Neil Roberts during Operation Anaconda in March 2002.
May 25, 1973	(50) Skylab 2, the first U.S. manned orbiting space station, launches with an all-Navy crew: Capt. Charles Conrad Jr., Cmdr. Paul J. Weitz, and Cmdr. Joseph P. Kerwin.
May 25, 2018	(5) Independence-variant littoral combat ship USS Manchester (LCS-14) is commissioned during a ceremony at the State Pier in Portsmouth, NH.
June 3, 1898	(125) During the Spanish-American War, seven men serving as a volunteer crew and the commander of USS Merrimac are taken as prisoners of war by the Spanish following a courageous attempt to sink the collier to obstruct navigation. For their “extraordinary heroism” during this operation, the men are awarded the Medal of Honor.
June 5, 2013	(10) USNS Millinocket (JHSV-3) is launched in Mobile, AL. The joint high-speed vessel is a noncombatant transport operated by Military Sealift Command.
June 7, 1898	(125) During the Spanish-American War, USS Marblehead (C-11), along with auxiliary cruisers USS Yankee and USS St. Louis, engage the Spanish gunboat Sandoval and the shore batteries at Guantanamo, Cuba for two and a half hours.
June 16, 1953	(70) During the Korean War, USS Princeton (CVS-37) launches 184 sorties against enemy front-line positions, a new record for offensive sorties flown from a carrier during the Korean War in a single day.
June 16, 2018	(5) Trilateral maritime exercise Malabar 2018 concludes. The exercise accomplished maritime interoperability training objectives among maritime forces from the United States, India, and Japan, emphasizing high-end warfighting skills, maritime superiority, and power projection. This was the first year that Malabar was conducted in the Guam operation area. The two-phase exercise took place ashore in Guam and underway in the Philippine Sea.
June 17, 1898	(125) President William McKinley signs into law a Congressional bill authorizing the establishment of the U.S. Navy Hospital Corps.



June 21, 1898	(125) During the Spanish-American War, the cruiser USS Charleston captures the island of Guam without resistance from Spain because the Spanish Navy had no sufficient ammunition for defense.
June 21, 2018	(5) The 13th annual Pacific Partnership mission concludes after mission stops in Japan and throughout South and Southeast Asia.
June 22, 1898	(125) During the Spanish-American War, the Spanish destroyer Terror joins Isabel II in an attempt to torpedo USS Saint Paul, which fires at Terror, damaging the ship.
June 22, 2018	(5) Lt. Christopher Carey Short is killed when the A-29 aircraft he was piloting crashed while on a mission over the Red Rio Bombing Range, part of White Sands Missile Range, north of Holloman Air Force Base in New Mexico.
June 23, 1898	(125) During the Spanish-American War, USS Dixie fires on two Spanish gunboats at Maria Aguilar Point, Cuba.
June 24, 1948	(75) The Berlin airlift "Operation Vittles" is initiated to offset the Soviet Union's blockade access of the United States, France, and Great Britain to their sectors of Berlin.
June 27, 1898	(125) During the Spanish-American War, the 301-ton yacht Hornet captures the Spanish steamer Benito Estenger off Cape Cruz, Cuba.
July 3, 1898	(125) During the Spanish American War, Rear Adm. Cervera's Spanish fleet attempts to flee from the harbor at Santiago, Cuba, but the U.S. Navy's Atlantic Squadron successfully pursues, attacks, and systematically destroys the Spanish vessels.
July 6, 1898	(125) During the Spanish-American War, the auxiliary-cruiser USS Dixie captures the Spanish vessels, Three Bells, Pilgrim, and Greeman Castle, off Cape Cruz, Cuba.
July 7, 1798	(225) Congress rescinds treaties with France, and the Quasi War begins.
July 7, 1948	(75) The first six enlisted women are sworn into the Regular Navy: Chief Yeoman Wilma J. Marchal; Yeoman Second Class Edna E. Young; Hospital Corpsman First Class Ruth Flora; Aviation Storekeeper First Class Kay L. Langen; Storekeeper Second Class Frances T. Devaney; and Teleman Doris R. Robertson.
July 11, 1798	(225) President John Adams signs an act that reestablishes the Marine Corps under the Constitution. The following day, Maj. William W. Burrows is appointed Commandant of the Marine Corps.
July 12, 2003	(20) USS Ronald Reagan (CVN-76) is commissioned at Naval Station Norfolk. The ninth in the Nimitz-class of nuclear-powered supercarriers, the ship's motto is "Peace through Strength," a phrase coined by President Reagan.
July 12, 2018	(5) Secretary of the Navy Richard V. Spencer inducts U.S. Sen. John S.



	McCain III into the official namesake of the guided-missile destroyer USS John S. McCain (DDG-56) in a ceremony on board the ship in Yokosuka, Japan.
July 17, 1898	(125) Santiago, Cuba surrenders to U.S. Naval forces during the Spanish-American War.
July 23, 1948	(75) During the Arab-Israeli War, USS Putnum (DD-757) evacuates the U.N. team from Haifa, Israel, and becomes first U.S. Navy ship to fly the U.N. flag.
July 25, 1898	(125) During the Spanish-American War, a landing party from the armed yacht USS Gloucester single-handedly captures Guanica, Puerto Rico.
July 25, 1998	(25) USS Harry S. Truman (CVN-75) is commissioned at Naval Station Norfolk, VA. The eighth aircraft carrier of the Nimitz-class is the first to be named after the 33rd president of the United States.
July 25, 2018	(5) Retired Rear Adm. Alene B. Duerk, the Navy's first female admiral, passes away. She was 98 years old.
July 26, 1948	(75) President Harry S. Truman signs Executive Order 9981, desegregating the Armed Services.
July 26, 2003	(20) USS Mustin (DDG-89) is commissioned at Naval Air Station North Island, CA. The Arleigh Burke-class guided-missile destroyer is the second to be named Mustin but the first to be named for the distinguished family of that name: Capt. Henry D. Mustin (1874–1923; Vice Adm. Lloyd M. Mustin (1911–1999); Vietnam War veteran Vice Adm. Henry C. Mustin II; and Lt. Cmdr. Thomas M. Mustin. The first USS Mustin, (DD-413) of the World War II era, was named for the family patriarch: Capt. Henry D. Mustin, who piloted the first aircraft ever catapulted from a ship and flew the first combat missions of American aircraft from Mississippi during the Mexican campaign in 1914.
July 27, 1953	(70) The Korean War armistice is signed at Panmunjon, Korea. The Korean cease-fire goes into effect at 22:00.
July 28, 1973	(50) Skylab 3 is launched. The mission is the second to the first U.S. manned space station. The commander of the mission is Capt. Alan L. Bean, USN; the pilot is Maj. Jack R. Lousma, USMC; and the science pilot is Owen K. Garriott, a former Navy electronics officer. The mission lasts 59 days, 11 hours and includes 858 Earth orbits. USS New Orleans (LPH-11) recovers the crew.
July 27, 2018	(5) Nimitz-class aircraft carrier USS Carl Vinson (CVN-70) rescues five mariners in distress July 27 near Hawaii's westernmost inhabited island.
July 29, 1898	(125) During the Spanish-American War, the gunboat USS Helena, commanded by Cmdr. William T. Swinburne, captures the Spanish steamer Manati at Cienfuegos, Cuba.
Aug. 2, 2018	(5) Exercise Rim of the Pacific, the world's largest international maritime



exercise, concludes following more than a month of training events conducted in and around the Hawaiian Islands and Southern California.

- Aug. 4, 1898 **(125)** During the Spanish-American War, USS Monterey (BM-6) becomes the first monitor to cross the Pacific, reaching Manila Bay, Philippines, from San Francisco, CA.
- Aug. 11, 1898 **(125)** During the Spanish-American War, USS Cushing (TB-1), USS Gwin (TB-16), and USS McKee (TB-18) capture and burn the Spanish schooner Jover Genard at Carendas, Cuba.
- Aug. 12, 1898 **(125)** USS Mohican and USS Philadelphia (C-4) crew members take part in official ceremonies marking the assumption of sovereignty of the Hawaiian Islands by the United States.
- Aug. 15, 1953 **(70)** Adm. Arthur W. Radford, USN, becomes the first naval officer to be appointed as the Chairman, Joint Chiefs of Staff, serving two terms until Aug. 15, 1957.
- Aug. 15, 1998 **(25)** USS Bonhomme Richard (LHD-6) is commissioned at Pensacola, FL. The Wasp-class amphibious assault ship is the third to honor the frigate used by Capt. John Paul Jones during the American Revolution.
- Aug. 24, 2018 **(5)** U.S. 2nd Fleet is reestablished during a ceremony aboard the nuclear aircraft carrier USS George H.W. Bush (CVN-77), at Naval Station Norfolk, VA, with Vice Adm. Andrew "Woody" Lewis as the commander.
- Aug. 25, 2018 **(5)** Former naval aviator, Vietnam War prisoner of war, and U.S. Senator John McCain passes away after a lengthy battle with cancer. He was 81.
- Aug. 29, 1998 **(25)** USS Decatur (DDG-73) is commissioned at Portland, OR. The Arleigh Burke-class guided missile destroyer is the fifth U.S. Navy ship named for Commodore Stephen Decatur.
- Aug. 29, 2018 **(5)** Chief of Naval Operations Adm. John Richardson selects Fleet Master Chief Russell Smith to be the 15th Master Chief Petty Officer of the Navy.
- Aug. 30, 1923 **(100)** USS Colorado (BB-45) is commissioned. Notable during her pre-WWII service, she helps in the search for missing aviator, Amelia Earhart, in 1937. During WWII, Colorado serves in the Pacific and in Leyte Gulf is hit by kamikazes November 1944.
- Aug. 30, 2018 **(5)** Guided-missile destroyer USS Jason Dunham (DDG-109) seizes an illicit shipment of arms from a stateless skiff in the international waters of the Gulf of Aden.
- Sept. 5, 1923 **(100)** The U.S. Asiatic Fleet arrives at Yokohama, Japan, to provide medical assistance and supplies after the Great Kanto earthquake, which occurred just days prior. On Sept. 1, during the earthquake, Lt. j.g. Thomas J. Ryan rescues a woman from the burning Grand Hotel in Yokohama. For his "extraordinary heroism" on that occasion, he is awarded the Medal of Honor.



Sept. 6, 1953	(70) The exchange of prisoners of war from Korean War called Operation Big Switch ends.
Sept. 7, 2013	(10) USS Minnesota (SSN-783) is commissioned at Naval Station Norfolk. The submarine, homeported at Groton, CT, is the 10th of the Virginia-class submarines and the third Navy vessel to be named after the state of Minnesota.
Sept. 8, 1923	(100) At Honda Point, CA, seven destroyers are run aground due to bad weather, strong currents, and faulty navigation. Twenty-three lives are lost during the disaster.
Sept. 16, 1823	(200) Samuel Southard becomes the seventh Secretary of the Navy, serving until March 3, 1829. During his tenure, he enlarges the Navy, improves administration, purchases land for the first naval hospitals, begins construction of the first Navy dry docks, undertakes surveying U.S. coastal waters, and promotes exploration in the Pacific Ocean.
Sept. 26, 1953	(70) The governments of the United States and Spain agree to establish a joint U.S.-Spanish naval facility at Rota in the Bay of Cadiz. The facility officially opens April 14, 1958.
Sept. 28, 2018	(5) U.S. Navy Sailors assigned to Underwater Construction Team (UCT) 2 render immediate assistance to the passengers and crew of Air Niugini flight PX56, after it crashes into the lagoon near Chuuk, Federated States of Micronesia, International Airport.
Oct. 1, 2018	(5) USS Indiana, the third vessel to be named for the state, is commissioned in a ceremony at Port Canaveral, FL.
Oct. 4, 1998	(25) U.S. and Algerian navies conduct the first bilateral exercise—a search and rescue operation involving USS Mitscher (DDG-57)—since Algerian independence in 1962.
Oct. 7–8, 2018	(5) Off the coast of Somalia, the Arleigh Burke-class guided missile destroyer USS Decatur (DDG-73) renders assistance to seven distressed mariners, whose fishing boat had suffered an engine malfunction, rendering the vessel inoperable.
Oct. 9, 1873	(150) Lt. Charles Belknap calls a meeting of 15 officers at the U.S. Naval Academy to establish the U.S. Naval Institute for the purpose of disseminating scientific and professional knowledge throughout the Navy.
Oct. 10, 1923	(100) The first American-built rigid airship USS Shenandoah (ZR-1), powered by helium gas instead of hydrogen, is christened at Naval Air Station Lakehurst, NJ. On Sept. 3, 1925, USS Shenandoah encounters violent weather over southern Ohio and breaks up. Fourteen of her crew lose their lives in this tragedy.
Oct. 15, 1948	(75) The first women officers on active duty are sworn in as commissioned officers in the Regular Navy under the Women's Armed Services Integration Act of June 1948 by Secretary of the Navy John L. Sullivan: Capt. Joy



B. Hancock; Lt. Cmdr. Winifred R. Quick; Lt. Cmdr. Anne King; Lt. Cmdr. Frances L. Willoughby; Lt. Ellen Ford; Lt. Doris Cranmore; Lt. j.g. Doris A. Defenderfer; and Lt. j.g. Betty Rae Tennant.

- Oct. 18, 2003 **(20)** USS Chafee (DDG-90) is commissioned at Newport, RI. The first U.S. Navy ship named to honor John Hubbard Chafee, the late Senator from Rhode Island, who also served as Secretary of the Navy under President Nixon.
- Oct. 19, 2018 **(5)** For the first time in nearly 30 years, a U.S. aircraft carrier enters the Arctic Circle. USS Harry S. Truman (CVN-75) and its strike group conduct operations in the Norwegian Sea.
- Oct. 22, 2018 **(5)** The U.S. Navy commissions its first unmanned aircraft system test and evaluation squadron during a ceremony at Naval Air Station Patuxent River's Webster Outlying Field.
- Nov. 4, 1923 **(100)** Lt. Alford J. Williams, flying an R2C-1 equipped with a Curtiss D-12 engine, raises the world speed record to 266.59 mph at Mitchel Field, Long Island, NY, beating the record set by Lt. Harold J. Brow only two days before.
- Nov. 5, 2018 **(5)** No one is injured when U.S. EP-3 Aries aircraft flying in international airspace over the Black Sea is intercepted by a Russian SU-27. During the unsafe interaction, the SU-27 conducts a high-speed pass directly in front of the mission aircraft, putting the crew at risk. The intercepting SU-27 made an additional pass, closing with the EP-3 and applying its afterburner while conducting a banking turn away.
- Nov. 7, 1973 **(50)** The War Powers Resolution becomes law. The law requires the president to notify Congress within 48 hours of committing armed forces to military action and forbids armed forces from remaining for more than 60 days, with a further 30-day withdrawal period, without an authorization of the use of military force or a declaration of war.
- Nov. 12, 2018 **(5)** A Carrier Air Wing (CVW) 5 F/A-18 experiences a mechanical issue that results in the crew ejecting while conducting routine operations in the Philippine Sea. The crew is immediately and safely recovered by USS Ronald Reagan (CVN-76) search and rescue aircraft.
- Nov. 16, 1798 **(225)** Off Havana, the warship Baltimore is halted by the British, who intend to impress Baltimore crewmembers who cannot prove American citizenship. Fifty-five seamen are imprisoned; 50 are later freed.
- Nov. 16, 1973 **(50)** Skylab 4 is launched, LTC Gerald P. Carr, USMC in command. The mission lasted 84 days and included 1,214 Earth orbits. Recovery by USS New Orleans (LPH-11).
- Nov. 17, 2018 **(5)** Littoral combat ship USS Sioux City (LCS-11) is commissioned during a ceremony at the U.S. Naval Academy.
- Nov. 27, 2018 **(5)** USS John S. McCain (DDG-56) achieves a major milestone as it



successfully launches from dry dock and moors pier side at Commander, Fleet Activities Yokosuka. The ship had been in drydock for about nine months following its collision with the merchant vessel Alnic MC while underway east of the Straits of Malacca and Singapore on Aug. 21, 2017.

- Nov. 30, 2018 **(5)** Former naval aviator and ex-President George H.W. Bush dies at age 94.
- Dec. 1, 2013 **(10)** Pilots and Sailors of VP-16 arrive on station at Kadena Air Base Okinawa for the first deployment of the P-8A Poseidon aircraft. The P-8A eventually replaces the venerable P-3 Orion.
- Dec. 3, 2018 **(5)** The Arleigh Burke-class guided missile destroyer, USS Thomas Hudner (DDG-116), is commissioned during a ceremony in Boston.
- Dec. 4, 1998 **(25)** USS Donald Cook (DDG-75) is commissioned at Philadelphia, PA. The ship is named in honor of the late Marine Corps Colonel Donald G. Cook, who was posthumously awarded the Medal of Honor for heroism in Vietnam while held as prisoner for three years by the Viet Cong.
- Dec. 6, 2018 **(5)** Naval aviators from various commands under Commander, Strike Fighter Wing Atlantic and Commander, Naval Air Force Atlantic, operating out of Naval Air Station Oceana, fly a 21-jet missing man formation over the George Bush Library and Museum at the interment ceremony for the late President George H.W. Bush.
- Dec. 12, 2018 **(5)** The Missile Defense Agency and U.S. Navy Sailors manning the Aegis Ashore Missile Defense Test Complex at the Pacific Missile Range Facility at Kauai, HI, successfully conduct an operational live fire test. The test demonstrates the Aegis weapon system “engage on remote” capability to track and intercept an Intermediate Range Ballistic Missile target with an Aegis Ashore-launched Standard Missile-3 (SM-3) Block IIA interceptor.
- Dec. 12, 2018 **(5)** Flying F-35C Lightning II aircraft, the “Argonauts” of Strike Fighter Squadron (VFA) 147 complete carrier qualifications aboard USS Carl Vinson (CVN-70), the final required component for Commander, Joint Strike Fighter Wing to issue the squadron its safe-for-flight operations certification.
- Dec. 16, 1998 **(25)** In Operation Desert Fox, Navy cruise missiles attack Iraq to degrade Saddam Hussein’s ability to make and use weapons of mass destruction.
- Dec. 29, 1798 **(225)** Secretary of Navy Benjamin Stoddert sends in his first annual report to Congress, requesting naval forces be increased “to make the most powerful nation desire our friendship—the most unprincipled respect our neutrality.”
- Dec. 31, 1948 **(75)** The last annual report by a Secretary of the Navy to Congress and the President is filed by Secretary of the Navy John L. Sullivan. Thereafter the Secretary of Defense reports annually to Congress.



APPENDIX K: POLITICAL ACTIVITY

Overarching Guidance

The U.S. Office of Special Counsel (OSC) routinely receives questions from federal employees and others about when the use of social media could violate the Hatch Act. Social media platforms are easily accessible to most employees while at work — on computers, smartphones, or other devices. OSC has created this guidance to help federal employees understand what the Hatch Act does and does not allow when using social media.¹

In general, all federal employees may use social media and comply with the Hatch Act if they remember the following three prohibitions:

- (1) On Duty or in the Workplace Prohibition — Employees may not engage in political activity while on duty or in the federal workplace.
- (2) 24/7 Prohibition — Employees may not knowingly solicit, accept, or receive a political contribution for a political party, candidate in a partisan race, or partisan political group.
- (3) 24/7 Prohibition — Employees may not use their official authority or influence to affect the outcome of an election.

Some employees are considered “further restricted” under the Hatch Act.² In addition to the three prohibitions above, further restricted employees are subject to a fourth prohibition:

- (4) 24/7 Prohibition — Further restricted employees may not take an active part in partisan political management or campaigning.

As such, further restricted employees may not engage in political activity on behalf of or in concert with a political party, candidate in a partisan race, or partisan political group. For instance, taking an “active part” would include: distributing material created by a political party, candidate in a partisan race, or partisan political group; speaking at a political rally organized or sponsored by such entities; or serving as a campaign volunteer.

This guidance will discuss each of the above prohibitions in turn. The last prohibition discussed is applicable only to further restricted employees. There are some very limited exceptions to these prohibitions for certain employees in specific positions and, when in doubt, employees are encouraged to contact OSC at hatchact@osc.gov or (202) 804-7002 with any additional questions.

1 This Hatch Act Guidance supersedes OSC’s prior guidance on social media in 2012 and 2015.

2 You are a further restricted employee under the Hatch Act if you are a career member of the Senior Executive Service, an administrative law judge, a contract appeals board member, an administrative appeals judge, or if you work in one of the following agencies, or agency components: (1) Central Intelligence Agency; (2) Criminal Division of the Department of Justice; (3) Defense Intelligence Agency; (4) Election Assistance Commission; (5) Federal Bureau of Investigation; (6) Federal Election Commission; (7) Merit Systems Protection Board; (8) National Geospatial- Intelligence Agency; (9) National Security Agency; (10) National Security Council; (11) National Security Division of the Department of Justice; (12) Office of Criminal Investigation of the Internal Revenue Service; (13) Office of the Director of National Intelligence; (14) Office of Investigative Programs of the United States Customs Service; (15) Office of Law Enforcement of the Bureau of Alcohol, Tobacco, and Firearms; (16) Office of Special Counsel; or (17) Secret Service. See 5 U.S.C. § 7323(b)(2)-(3).



(1) ON DUTY OR IN THE WORKPLACE PROHIBITION – Employees may not engage in political activity while on duty or in the workplace.³ Political activity is an activity directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

(A) Posting, Liking,⁴ Sharing, or Retweeting Partisan Messages

Rule: Employees may not post, like, share, or retweet a message or comment in support of or opposition to a political party, candidate in a partisan race, or partisan political group while on duty or in the workplace, even if their social media account is private.

Example 1: You are at home after work. You may like or tweet a message encouraging others to vote for your favored candidate in a partisan race.

Example 2: You are on duty and looking at Facebook on your personal cell phone. You see that a friend posted a message encouraging others to vote for members of a certain political party. You may not like or share that message while you are on duty.

Example 3: You stay at work during your lunch break and check Facebook on your personal cell phone. A Facebook friend posted a message about an upcoming event supporting a candidate in a partisan race. Even if you are not in a pay status during your lunch break, you may not like or share that post while you are in the workplace.

Example 4: You are teleworking from home and on your lunch break in which you are not in a pay status. You are looking at Facebook on your personal iPad and see that a friend posted a message about an upcoming event supporting a political party. Because you are on your lunch break and not in a federal building, you may like or share that post.

Example 5: You are teleworking from home and looking at Twitter on your personal computer. You see that the President tweeted an endorsement of a congressional candidate. You may not like or retweet that message while on duty.⁵

Example 6: You are teleworking and looking at Facebook on your personal cell phone. You see that a Senate candidate posted a message asking for votes on Election Day. You may not post a comment in support of that message while on duty.

(B) Liking, Following, or Friending Candidates or Partisan Groups

Rule: Employees may not like, follow, or friend the social media account of a political party, candidate in a partisan race, or partisan political group while on duty or in the workplace.

Example 1: You are at home after work and find the Instagram account of a partisan political group. You may follow them on Instagram and like their posts.

Example 2: You are at work and looking at your private Facebook account on your personal iPad. A Facebook friend shared the post of a candidate in a partisan race announcing that he or she received an endorsement. You may not like, follow, or friend the candidate's Facebook page while on duty or in the workplace.

(C) Liking, Following, or Friending the Official Social Media Accounts of Government Officials

³ Employees also may not engage in political activity while wearing a uniform or official insignia identifying the office or employee's position, or while using a government owned or leased vehicle.

⁴ Liking includes the use of other emojis or reactions, such as those in the "like" function of Facebook.

⁵ The President and Vice President are not covered under the Hatch Act and, as a result, are not subject to its social media restrictions.



Rule: Employees may continue to follow, be friends with, or like the official social media accounts of government officials after those officials become candidates for reelection.

Example 1: You follow the official government Twitter account of the President or a Member of Congress, who has just announced their candidacy for reelection. You may continue to follow these official accounts.

(D) Using an Alias on Social Media

Rule: Employees may not use an alias on social media to engage in any activity that is directed at the success or failure of a political party, candidate in a partisan race, or partisan political group while on duty or in the workplace.

Example 1: Your name is John Smith, but you create a Facebook profile as John Jones. You are at home after work and see that a Facebook friend posted a negative message about a candidate in a partisan race. You may share or like that post.

Example 2: Your name is Jane Smith, but you create a Twitter account as Jane Jones. You are at work, on duty, and looking at your alias Twitter account on your personal cell phone. An actor you follow on Twitter posted a negative message about a political party. You may not like or retweet that message either as Jane Smith or Jane Jones while on duty or in the workplace.

(E) Profile Pictures on Social Media Accounts

Rule: Employees may display a political party or current campaign logo or the photograph of a candidate in a partisan race as a profile picture on personal Facebook or Twitter accounts; however, they may not post, share, tweet, or retweet on those accounts while on duty or in the workplace.⁶

Example 1: You decide to use a current campaign logo as your profile picture on your personal Twitter account. Although you may use the logo as your profile picture, you may not tweet or retweet any messages on that account while on duty or in the workplace.

(F) Cover and Header Photographs on Social Media Accounts

Rule: Employees may display a political party or campaign logo or photograph of a candidate in a partisan race as a cover or header photograph on their personal Twitter or Facebook accounts.⁷

Example 1: You recently took a photograph with a candidate in a local partisan race. You may use the photograph as the header on your personal Facebook account.

(2) 24/7 PROHIBITION – Employees may not knowingly solicit, accept, or receive a political contribution for a political party, candidate in a partisan race, or partisan political group.

(A) Posting or Tweeting Solicitations

⁶ Because a profile picture accompanies most actions on social media, employees would not be permitted, while on duty or in the workplace, to post, share, tweet, or retweet any items on Facebook or Twitter, because each such action would show their support for a political party, candidate in a partisan race, or partisan political group, even if the content of the post, share, tweet, or retweet is not about those entities.

⁷ Unlike profile pictures, cover and header photographs do not accompany most actions on social media. Therefore, the Hatch Act generally does not prohibit employees from using their social media accounts at work, even if they display a political party or campaign logo or photograph of a candidate in a partisan race as their cover or header photograph. But employees should always consult their agency's computer-use policies before using any social media at work.



Rule: Employees, even when not on duty or in the workplace, may not post or tweet a message that solicits political contributions or invites people to a fundraising event.

Example 1: You may not tweet a message asking your Twitter followers to contribute five dollars to help a candidate in a local partisan race.

Example 2: You are attending a political party's annual fundraising event. You may not post a message on Facebook inviting friends to join you at the event.

(B) Liking, Sharing, or Retweeting Solicitations

Rule: Employees, even when not on duty or in the workplace, may not like, share, or retweet a post that solicits political contributions, including invitations to fundraising events.

Example 1: Someone tweets a message offering to match the donation of the first five friends that donate to a certain candidate in a local partisan race. Although the Hatch Act does not prohibit you from donating to the campaign, you may not like, share, or retweet that post.

Example 2: A friend shares a post on Facebook that includes an invitation to a local fundraising event for a political party. You may not like or share that post.

Example 3: Someone tags you in a post, or posts a message to your Facebook page, that asks for donations for a partisan political group. You do not have an affirmative duty to remove that post from your Facebook page or un-tag your name from the post; however, you may not like or share the post.

(C) Accepting Invitations to Fundraising Events on Social Media

Rule: If not on duty or in the workplace, employees may accept invitations to, or mark themselves as "attending," a fundraising event on social media.

Example 1: A friend sends you an invitation on Facebook to a fundraising event for a candidate in a partisan race. You may accept the invitation or mark yourself as "attending" the fundraising event, provided you are not on duty or in the workplace.

(D) Using an Alias on Social Media

Rule: Employees, even when not on duty or in the workplace, may not use an alias on social media to solicit a political contribution for a political party, candidate in a partisan race, or a partisan political group.

Example 1: Your name is John Smith, but you create a Facebook profile as John Jones. You are at home after work and see that a Facebook friend posted a message that solicits campaign contributions for a candidate in a partisan race. You may not share that message either as John Smith or John Jones.

(3) 24/7 PROHIBITION – Employees may not use their official authority or influence to affect the outcome of an election.

(A) Using Official Title or Position in Social Media Profile

Rule: Employees may include their official titles or positions and where they work in their social media profiles, even if they also include their political affiliation or otherwise use their account to engage in political activity.

Example 1: Your Twitter profile includes your official title or position and where you work. You



may also list your political affiliation.

Example 2: Your Facebook profile includes your official title or position, where you work, and your political affiliation. You may post a message supporting a candidate in a partisan race, provided you are not on duty or in the workplace.

(B) Using Official Title or Position in Social Media Communications

Rule: Employees may not use their official titles or positions when posting messages directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

Example 1: While at home after work, you decide to post a positive comment on the Twitter account of a candidate in a local partisan race. You may not mention your official title or position in that comment, even if your Twitter account is private.

Example 2: Your LinkedIn profile headline includes your official title or position. You may not use that LinkedIn account to post or share messages directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.⁸

(C) Using Official Social Media Accounts

Rule: Employees may not use a social media account designated for official purposes to post or share messages directed at the success or failure of a political party, candidate in a partisan race, or partisan political group. All such official social media accounts should remain politically neutral.

Example 1: While accessing the Twitter account you use for official purposes, you see that a political party tweeted its support for a candidate in a partisan race. You may not retweet or like that post from the account used for official purposes (or from your personal social media account if you are on duty or in the workplace).

(D) Misusing Personal Social Media Accounts

Rule: Employees may not engage in political activity on a personal social media account if they are using such accounts for official purposes or posting in their official capacities. Factors indicating that a personal social media account is being used in ways that suggest it is an official social media account include, for example: (1) the account contains little to no personal content; (2) the account identifies the individual as a federal employee; (3) the account extensively uses photographs of the employee's official activities; (4) the account often references, retweets, likes, comments, or otherwise shares material related to official activities; or (5) the account is linked to an agency website or other official page. No one factor is dispositive.

Example 1: You are a federal employee and maintain only a personal Twitter account. While you have some personal posts about family vacations and events with friends, most of your posts are retweets of your agency's initiatives and photographs of you at official events. You may not use this account to make posts directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

⁸ A LinkedIn profile headline accompanies most actions on LinkedIn. Therefore, employees who include an official title or position in their LinkedIn profile headline would not be permitted to post or share any messages on LinkedIn that are directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.



(E) Targeting Subordinates and Certain Groups⁹ in Social Media Communications

Rule: Supervisors and subordinates may be friends or follow one another on social media platforms. However, supervisors may not send to subordinates, or to a subset of friends that includes subordinates, any message that is directed at the success or failure of a political party, candidate in a partisan race, or partisan political group.

Example 1: You are a supervisor. You may tweet generally about your support of a candidate in a local partisan race even if one of your subordinates follows you on Twitter, provided you are not on duty or in the workplace.

Example 2: You are a supervisor. You may not mention, or use the Twitter handle of, a subordinate who follows you on Twitter when tweeting your support of a candidate in a partisan race.

Example 3: You are a supervisor. You want to send via Facebook Messenger your opinion about which candidate to support in an upcoming partisan election. You may not include a subordinate employee in the recipient group of that message.

(4) 24/7 PROHIBITION – *Further restricted employees* may not take an active part in partisan political management or campaigning.

(A) Sharing or Retweeting Partisan Messages

Rule: Further restricted employees may not share or retweet posts from, or the page of, a political party, candidate in a partisan race, or partisan political group, even if they are not on duty or in the workplace.

Example 1: You are at home using your personal cell phone to look at Facebook. You see that a political party has posted a message about voting on Election Day. You may not share that post.

Example 2: You may like the campaign Facebook page of a candidate in a partisan race, but you may not share that page.

Example 3: A friend has shared a Facebook post from the campaign of a Presidential candidate. You may not share that post.

(B) Linking to Partisan Material or Websites

Rule: Further restricted employees may not link to campaign or other partisan material of a political party, candidate in a partisan race, or partisan political group, even if they are not on duty or in the workplace.

Example 1: You may not include in your Facebook profile the link to the website of a candidate in a partisan race.

Example 2: You may not tweet a message in support of a candidate in a partisan race that includes a link to that candidate's Twitter account.

(C) Posting to or Liking Partisan Social Media Accounts or Messages

Rule: Further restricted employees may post to or like the social media accounts or messages

⁹ The Hatch Act prohibits an employee from knowingly soliciting or discouraging the political activity of any person who, for example, has a grant application pending before, or is the subject of an investigation by, the employee's employing office.



of a political party, candidate in a partisan race, or partisan political group, provided they are not on duty or in the workplace.

Example 1: Your friend is running for Congress. You may like her campaign Facebook page or post a message of support on her page, provided you are not on duty or in the workplace.

(D) Posting Personal Political Opinions

Rule: While not on duty or in the workplace, further restricted employees may engage in political activity on social media, provided it is not done in concert with or on behalf of a political party, candidate in a partisan race, or partisan political group.

Example 1: You may tweet your own message advocating the defeat of a Presidential candidate, provided you are not on duty or in the workplace.

Guidance For Armed Forces

Q1. What is the DoD policy regarding political activities by members of the Armed Forces?

A1. DoD has a longstanding policy of encourage military personnel to carry out the obligations of citizenship. However, AD members will not engage in partisan political activities and all military personnel will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval or endorsement of a political candidate, campaign or cause.

Q2. Can political candidates visit a DoD installation or facility?

A2. A candidate for civil office may not be permitted to engage in campaign or election related activities (e.g., public assemblies, town hall meetings, speeches, fund-raisers, press conferences, post-election celebrations, and concession addresses) while on a DoD installation, which includes overseas installations and areas under the control of combat or peacekeeping forces of the United States military.

Q3. Can a seated politician visit a DoD installation or facility if they are campaigning for office?

A3. A candidate who holds a civil office may visit a DoD installation or facility for the purpose of conducting official business or to access entitlements or benefits the candidate is authorized to use; however, no candidate running for office is permitted access for campaign or election purposes.

Q4. How does DoD define when a political campaign begins and ends?

A4. According to DoD policy, a political campaign or election begins when a candidate, including an incumbent officeholder, makes a formal announcement to seek political office or when an individual files for candidacy with the Federal Election Commission or equivalent regulatory office. Once initiated, a political campaign or election does not end until one week after the conclusion of the relevant election.

Q5. What political activities can a service member participate in and which ones are prohibited?

A5. DoD has a longstanding policy of encouraging military personnel to carry out the obligations of citizenship, and certain political activities are permitted, such as voting and making a personal monetary donation. However, active duty members will not engage in partisan political activities, and all military personnel will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval or endorsement of a political



candidate, campaign or cause.

Examples of political activities that are prohibited include campaigning for a candidate, soliciting contributions, marching in a partisan parade and wearing the uniform to a partisan event. For a complete list of permissible and prohibited activities, please consult

DoD Directive 1344.10, Political Activities by Members of the Armed Forces Guidance for Military Personnel.

Q6. Does that mean a service member can vote, but not actively support a particular candidate or cause?

A6. Unquestionably, service members can exercise their right to vote. However, AD members will not engage in partisan political activities and will avoid the inference that their political activities imply or appear to imply DoD sponsorship, approval, or endorsement. For a list of permissible and prohibited activities, please consult DoD Directive 1344.10, Political Activities by Members of the Armed Forces (reference (c)).

Q7. Does DoD support and encourage its personnel to vote?

A7. DoD encourages all members of the Armed Forces and federal civilian employees to register and vote. The department actively supports the Federal Voting Assistance Program to ensure its personnel have the resources, time and ability to participate in their civic duty. Additionally, department leaders and military commanders appoint voting assistance officers at every level of command and ensure they are trained and equipped to provide voting assistance.

Q8. Can a DoD installation be used as a polling place in an election?

A8. As of December 31, 2000, if an installation facility is designated as an official polling place by an election official or has been used as a polling place since January 1, 1996, installation commanders will not deny the use of that facility as a polling place for any election. The Secretary of Defense or the secretary of the military department concerned may grant a waiver of the requirement to allow use of the facility if it is determined that security is a concern. All members of the Armed Forces on AD are instructed to remain clear of all polling places except when voting.

Q9. Does DoD provide any voting assistance?

A9. Yes, DoD provides voting assistance via the Federal Voting Assistance Program. FVAP works to ensure service members, their eligible family members and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so – from anywhere in the world – via FVAP.gov. The services also provide voting assistance officers at the unit level to facilitate in-person assistance when required.

Guidance For Civilians

Before posting about politics on social media, Department of the Navy civilians need to consider the Hatch Act and DoD policy.

In general, as a federal employee, you may use social media and comply with the Hatch Act if you:

- Don't engage in political activity while on duty or in the workplace, even if you're using your



personal smartphone, tablet, or laptop to do so. Federal employees are “on duty” when they’re in a pay status (including during telework hours, but not including paid leave) or are representing the government in an official capacity.

- Don’t post political opinions, likes, shares, etc. while on government property, even if inside your vehicle on a lunch break, using your own device to post to your personal account.
- Don’t engage in political activity in an official capacity at any time. Political activity refers to any activity directed at the success or failure of a political party or partisan political group or candidate in a partisan race.
- Don’t solicit or receive political contributions at any time.

As a civilian, you may express your opinions about a partisan group or candidate in a partisan race by posting, liking, sharing, tweeting or retweeting, but there are a few limitations. The Hatch Act prohibits federal employees from:

- Referring to your official titles or positions while engaged in political activity at any time; it’s important to note that including your official title or position in your social media profile is not an improper use of official authority.
- Suggesting or asking anyone to make political contributions at any time, including providing links to the political contribution page of any partisan group or candidate in a partisan race or liking, sharing or retweeting a solicitation from one of those entities.
- Liking, sharing or retweeting an invitation to a political fundraising event; however, you may accept an invitation to a political fundraising event from such entities via social media.
- Posting political opinions/likes/shares while on government property, even if inside your vehicle on a lunch break, using your own device to post to your personal account.

Civilians who fall in the “further restricted employees” category may express opinions about a partisan group or candidate in a partisan race by posting or sharing content, but there are a few limitations. In addition to the limitations above, the Hatch Act prohibits further restricted employees from:

- Posting or linking to campaign or other partisan material of a partisan group or candidate in a partisan race. Sharing those entities’ social media sites or their content, including retweeting.

Civilians are allowed to identify their political party affiliation in their social media profiles, even if the profile also contains their official title or position, without more. As a civilian, you may display a political party or campaign logo or a candidate photograph in your profile picture, but it’s subject to the following limitations: Because a profile picture accompanies most actions on social media, while in the workplace you would not be permitted to post, share, tweet, or retweet any partisan social media content because each such action would show your support for a partisan group or candidate in a partisan race, even if the content of the action is not about those entities.

For the full policy and more details, see the U.S. Office of Special Counsel website at: <http://www.osc.gov>





DoD INSTRUCTION 5400.17

OFFICIAL USE OF SOCIAL MEDIA FOR PUBLIC AFFAIRS PURPOSES

Originating Component:	Office of the Assistant to the Secretary of Defense for Public Affairs
Effective:	August 12, 2022
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/ .
Approved by:	Gordon Trowbridge, Acting Assistant to the Secretary of Defense for Public Affairs

Purpose: In accordance with the authority in DoD Directive (DoDD) 5122.05 and DoD Instruction (DoDI) 8170.01, this issuance:

- Establishes policies and provides procedures:
 - For initiating an external official presence (EOP) on social media platforms for public affairs (PA) purposes.
 - To maintain an EOP on social media platforms.
- Assigns responsibility to OSD and DoD Components for EOP on social media platforms.
- Provides:
 - Core principles regarding social media use within DoD.
 - Guidance regarding records management procedures for social media accounts.
 - Guidance on personal social media use by DoD personnel.



TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION	4
1.1. Applicability.	4
1.2. Policy.	4
SECTION 2: RESPONSIBILITIES	5
2.1. Assistant to the Secretary of Defense for Public Affairs (ATSD(PA)).	5
2.2. DoD Chief Information Officer.	5
2.3. OSD and DoD Component Heads.	6
SECTION 3: CORE PRINCIPLES OF SOCIAL MEDIA USE WITHIN DoD	7
3.1. Official Use of Social Media.	7
3.2. DoD Social Media Principles.....	7
a. Governance.	7
b. Professionalism.	7
c. Propriety.....	8
d. Acumen.	8
e. Establishment Need.....	8
f. Transparency.	8
SECTION 4: DoD EOP	9
4.1. Establishing An Official Presence.	9
a. Considerations Concerning Official Accounts.....	9
b. Registering an Account.	10
c. Establishing EOPs for OSD and DoD Component Heads.	10
d. EOPs Below the Component Level.	10
4.2. New and Emerging Platforms.	11
SECTION 5: BRANDING GUIDELINES.....	12
5.1. Clear Identification.	12
5.2. Official DoD and Military Department and Service Seals vs. Emblems and Logos.....	12
SECTION 6: AUTHORIZED ACCOUNTS.....	13
6.1. Official Social Media Conduct.	13
6.2. PA Official Use of Social Media.	15
a. Official Organizational Accounts.	15
b. Official Institutional Accounts.....	15
c. Official Individual Accounts.....	16
6.3. Military Marketing and Recruitment Accounts.	16
SECTION 7: MAINTAINING AN EOP	17
7.1. Records Management.....	17
a. DoD Information Security.....	17
b. Managing Social Media Records.	17
c. Capturing Social Media.....	17
d. Private or Direct Messages from DoD Social Media Accounts.	18
e. Account Transition and Archiving of Official Social Media Accounts.....	18
7.2. Use of PAI For PA.	19
7.3. Risks Associated with Operating EOP.	20
a. Social Media Cyber-Vandalism.	20

b. Fake or Imposter Social Media Accounts of DoD Employees and Service Members.	20
7.4. Linking and Sharing from Official Social Media Accounts.	21
7.5. Social Media Platform Verified Accounts.....	22
SECTION 8: PERSONAL SOCIAL MEDIA USE BY DoD PERSONNEL.....	23
a. Maintain a Clear Distinction Between Personal and Official Accounts.	23
b. Do Not Disclose Non-Public Information.	23
c. Do Not Conduct Official Business on Personal Social Media Accounts.....	24
d. Do Not Accept Compensation for any Activity Relating to One’s Status as a DoD Civilian Employee or Military Service Member.....	24
e. Do Not Engage in Prohibited Political Activity, as Defined in Applicable Law and Regulation.	24
GLOSSARY	25
G.1. Acronyms.	25
G.2. Definitions.....	25
REFERENCES	27
FIGURES	
Figure 1. Mandatory Acceptable Use Policy Agreement Statements.....	10
Figure 2 Sample Disclaimer for Personal Social Media Accounts.....	23

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance:

(1) Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the “DoD Components”).

(2) Does not apply to social media accounts established for marketing activities by Military Service recruiting commands, in accordance with DoDI 1304.35.

b. Nothing in this issuance should be construed as preventing the Inspector General of the Department of Defense from fulfilling their duties pursuant to Sections 7321-7326 of Title 5, United States Code (U.S.C.), Appendix, also known as the Inspector General Act of 1978, as amended.

1.2. POLICY.

a. It is DoD policy to use official DoD accounts on non-DoD controlled social media platforms to amplify timely and relevant information about the national security, defense strategy, and appropriate unclassified work of the Department.

b. It is DoD policy that:

(1) The ability to adapt to changing trends and technologies on dynamic social media platforms is needed to take full advantage of social media as a communication tool and in support of the National Defense Strategy in accordance with Section 113(g) of Title 10, U.S.C.

(2) The integration of social media is an integral element of DoD strategies to communicate official information publicly in accordance with DoDI 8170.01.

(3) Information communicated by OSD and DoD Components on official social media accounts constitutes a segment of PA activities, in accordance with DoDI 5400.13, DoDD 5122.05, and this issuance.

(4) Information disclosed will be in compliance with the DoD Principles of Information in accordance with DoDD 5122.05.

SECTION 2: RESPONSIBILITIES

2.1. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS (ATSD(PA)).

The ATSD(PA):

- a. Is the principal spokesperson for DoD and responsible for ensuring a free flow of information to the news media, general public, internal audiences of DoD, and other applicable forums through official DoD social media accounts managed by OSD and DoD Components, in accordance with DoDD 5122.05.
- b. Provides the final approval for all EOPs established by OSD and DoD Component heads in accordance with DoDI 8170.01 concerning the use of social media.
- c. May direct the removal of any official social media account that does not adhere to the policy, procedures, and instructions provided in this issuance.
- d. Oversees the implementation of integrated communication strategies that incorporate digital media content on official DoD social media accounts.
- e. Provides guidance and direction for OSD and DoD Components to use publicly available information (PAI) for PA activities through third-party social media management platforms, in accordance with DoDD 3115.18.
- f. Ensures the conduct of appropriate pre-publication security and policy reviews in accordance with DoDIs 5230.09 and 5230.29, as applicable.

2.2. DOD CHIEF INFORMATION OFFICER.

The DoD Chief Information Officer:

- a. In coordination with ATSD(PA), oversees implementation of policy and procedures for ensuring the quality of information the DoD disseminates to the public.
- b. On a limited, case-by-case basis, reviews requests by OSD and DoD Component heads to negotiate terms of service with a non-DoD controlled electronic messaging service. In coordination with the ATSD(PA), Chief Digital and Artificial Intelligence Officer, and DoD Office of General Counsel, the DoD Chief Information Officer reviews the request in accordance with DoDI 8170.01.

2.3. OSD AND DOD COMPONENT HEADS.

The OSD and DoD Component heads:

- a. May establish EOPs for their Components, in accordance with the provisions of Section 4.
- b. May establish Component-specific social media regulations to manage social media managers, accounts, and activities.
- c. For any EOP they establish, ensure proper management of records created or received through activity of the EOP throughout the lifecycle of the records in accordance with DoDI 5015.02.

SECTION 3: CORE PRINCIPLES OF SOCIAL MEDIA USE WITHIN DoD

3.1. OFFICIAL USE OF SOCIAL MEDIA.

a. Social media communication provides the opportunity and responsibility to communicate directly to the public. DoD uses official social media accounts for the sake of transparency and to disseminate information.

b. If social media is mismanaged or mishandled, the U.S. Government's reputation with the American public; relationships with interagency, international, State, local, and tribal entities; military operations; and reputation for a high ethical and professional standard may be compromised. DoD social media content can be consumed by any audience, intended or unintended, foreign or domestic. All DoD PA and social media managers should understand that even the smallest or newest official account will be interpreted as a representative of the whole of DoD.

c. DoD personnel may establish accounts for personal, non-official use in accordance with DoDI 8170.01. Personal accounts may not be used to conduct official DoD communications, unless by exception identified in Paragraph 3.26.a of DoDI 8170.01. DoD personnel must ensure that their personal social media accounts avoid use of DoD titles, insignia, uniforms, or symbols in a way that could imply DoD sanction or endorsement of the content. Where confusion or doubt is likely to arise regarding the personal nature of social media activities, personnel are encouraged to include a disclaimer clarifying that their social media communications reflect only their personal views and do not necessarily represent the views of their agency or the United States. See Section 8 of this instruction for additional guidance on the personal use of social media by DoD personnel.

3.2. DOD SOCIAL MEDIA PRINCIPLES.

The following principles will apply to official use of social media for PA purposes:

a. Governance.

OSD and DoD Component PA teams oversee and provide guidance on the use and management of official DoD social media accounts. Communications will align with and support PA objectives and efforts across all platforms.

b. Professionalism.

All official social media content is a reflection of the Department. When posting to official social media accounts, content should meet well-defined, appropriate objectives. Public Affairs Officers will remain respectful, responsive, and genuine, and exercise the same high standard of professional and ethical behavior on social media accounts as they do during any other function or on any other platform. Content should inspire and engage with audiences. At no time, however, should such content undermine the Department's efforts to remain a good steward of the public trust. No content will be released that could be reasonably construed as offensive, inappropriate, or unbecoming. Official social media accounts must not be used to promote or

endorse non-Federal entities or personal financial interests. Only designated DoD personnel may authorize release of information on social media accounts; contractor personnel may support EOP maintenance but cannot authorize the release of public information.

c. Propriety.

Posts released from official DoD social media accounts must be:

- (1) Accurate. The content is accurate.
- (2) Appropriate. The account is the proper vehicle for the message.
- (3) Timely. The message can be delivered at the proper time.
- (4) In the Appropriate Tone. The message is being delivered in the proper tone.
- (5) Approved for public release. The message has been reviewed for operations security and information security concerns and approved for public release, in accordance with DoDIs 5230.09 and 5230.29, as applicable.

d. Acumen.

PA officers and social media account managers should proactively maintain currency in the latest social media tactics, best practices, and trends, coupled with an understanding of and ability to apply PA objectives (e.g., as articulated in the DoD Communications Playbook). Social media account managers must complete operations security training Level 2 and be prepared to act quickly and implement evolving capabilities intelligently to remain effective in the use of the platform.

e. Establishment Need.

New official accounts should only be established if a specific communications outcome cannot be fulfilled by an existing account(s) or other means of communication. More for the sake of more is not necessarily better.

f. Transparency.

Social media account managers will not remove social media content from official DoD accounts unless there is a factual or typographical error; violation of a law, policy, term of service, or user agreement; or an operations or information security concern. Removal of content will be publicly acknowledged and communicated to audiences to provide context and appropriate clarification for the action; managers must persistently monitor, communicate, and, where appropriate, responsively engage with users regarding such removal. Removal of content can unintentionally discredit DoD information if the action appears to be taken to:

- (1) Avoid embarrassment;
- (2) Stifle or silence discussion about a controversial topic; or
- (3) Mislead users to believe an issue is inconsequential or of minor significance.

SECTION 4: DoD EOP

4.1. ESTABLISHING AN OFFICIAL PRESENCE.

a. Considerations Concerning Official Accounts.

(1) OSD and DoD Components must assess the communication value of establishing an official presence on approved social media platforms to provide timely and accurate information to the public and the news media in accordance with DoDD 5122.05 and Paragraph 3.24 of DoDI 8170.01.

(2) The creation of EOPs on social media platforms should be carefully considered and avoided, unless the proposed EOP meets a specific communications objective that is not being fulfilled by any existing EOP or other PA activities. Commands at all levels will consolidate and deactivate EOPs that detract or disrupt users searching for official DoD information. Content on any deactivated official accounts must be archived in accordance with DoDI 5015.02.

(3) Organizations that identify a communication need that can be satisfied through social media should evaluate available resources to establish and manage an account with the intent to build and engage audiences, and use analytics to elevate their digital impact.

(4) PA offices should be resourced with the industry standard equipment, training, and personnel to manage social media accounts, especially over multiple social media platforms, including public web activities pursuant to DoDD 5122.05.

(5) Pursuant to Paragraph 3.24.k. of DoDI 8170.01, mission-related contact information must be used to establish an EOP.

(6) DoD personnel managing or having access to an official social media account will coordinate with their local information technology offices and sign an acceptable use policy agreement for tracking purposes in accordance with Component cybersecurity regulations.

(7) Acceptable use policy agreements must include the statements in Figure 1. If the existing acceptable use policy agreement does not contain the language in Figure 1, it should be amended accordingly or a standalone acknowledgement containing the language in Figure 1 should be signed.

Figure 1. Mandatory Acceptable Use Policy Agreement Statements

I will use official DoD social media accounts on non-DoD-controlled social media platforms (e.g., Facebook, YouTube, Twitter, Instagram) only as authorized by my job or duty description and to conduct official business, including to release official agency information or other official communication. I will not use personal social media accounts to conduct official business except as authorized in accordance with DoDI 8170.01.

b. Registering an Account.

(1) All DoD owned and/or operated social media accounts must be registered at <https://www.defense.gov/Resources/Register-a-Site/> and must register with the U.S. Digital Registry at <https://www.digitalgov.gov/services/u-s-digital-registry/> in accordance with DoDI 8170.01.

(2) Registering accounts constitutes the official status for DoD social media accounts on authorized platforms.

c. Establishing EOPs for OSD and DoD Component Heads.

(1) In coordination with the ATSD(PA), OSD and DoD Component heads approve the creation of individual social media accounts for their positions. OSD and DoD Component heads will submit an action memo to the ATSD(PA) requesting the establishment of a new individual or institutional social media account.

(2) DoD personnel, including OSD and DoD Component heads and other military and civilian leaders, are prohibited from converting personal accounts to official DoD accounts associated with their DoD position, title, duty, component, or any other DoD organizational entity.

(3) OSD and DoD Component heads are authorized to close or archive any social media accounts deemed unnecessary and of no informational value to the public, media, or mission of the Component. The process to archive and close a social media account is provided in Paragraph 7.1.e.

d. EOPs Below the Component Level.

(1) OSD and DoD Component heads, in consultation with PA, will review and determine the criteria for establishing an EOP for elements within their responsibility to operate and execute their PA activities. PA representatives should assess establishing an EOP based on mission or operational needs and support of approved communication plans and campaigns.

(2) EOPs at all levels must follow the procedures, policies, and guidelines outlined in this issuance. Organizations that establish an EOP will provide guidance to social media managers to effectively direct activities and properly maintain the organization's public presence.

4.2. NEW AND EMERGING PLATFORMS.

a. PA and social media managers must consider the communication value of expanding their digital presence and conduct researched analysis of new platforms. Some of the elements that PA and social media managers should consider include, but are not limited to, audience analysis, content strategy for the platform, and available resources. Approving officials should obtain data-driven decisions from PA and social media managers and ensure compliance with Paragraph 3.24 of DoDI 8170.01 before accepting recommendations to expand their digital footprint.

b. The process to review platforms for official presence requires an application to be vetted through the Defense Information Systems Agency's DoD Application Vetting Environment. The application must be submitted after coordination with the Component Chief Information Officer to ensure all information provided is complete.

c. Once the DoD Application Vetting Environment review process is completed, the Defense Information Systems Agency will issue a decision. This decision is applicable for all OSD and DoD Components and is considered final.

d. PA and social media managers should **not** test, use, or otherwise engage on new platforms for official use (including on personal devices) prior to undertaking the steps in Paragraphs 4.2.a- c.

SECTION 5: BRANDING GUIDELINES

5.1. CLEAR IDENTIFICATION.

To maintain an EOP, all DoD Components will adhere to branding guidelines in accordance with DoDD 5535.09 and:

- a. Provide clear identification that they are supplying the content for the EOP.
- b. State their mission and provide the purpose of the EOP, as workable.
- c. Will not mislead users of the site as to the originator of the EOP.

5.2. OFFICIAL DOD AND MILITARY DEPARTMENT AND SERVICE SEALS VS. EMBLEMS AND LOGOS.

a. The use of the official DoD seal, official Military Department seals, and official Military Service seals on EOP accounts is reserved for official communication only, such as letterheads, and briefing documents. The use of DoD and Military Service emblems, logos, or coats of arms may be more appropriate for general use on EOPs to affiliate the account with DoD. Social media managers should reference Component guidance for the appropriate uses of Component marks for official social media use.

b. DoD and OSD Components should develop Component-specific guidance for the use of their emblems or logos on EOPs and social media content.

SECTION 6: AUTHORIZED ACCOUNTS

6.1. OFFICIAL SOCIAL MEDIA CONDUCT.

a. All EOPs and their content represent DoD, reflect the values of the Department, and serve as official communication platforms to the general public, the news media, and internal audiences of DoD. Content posted on official accounts is subject to the same guidance, policy, regulations, and oversight for the release of official DoD information.

b. PA chiefs and social media managers must establish communication planning techniques to ensure the information published on a social media account is synchronized and approved for release. Social media content management software and tools may be used for PA activities.

c. PA chiefs, social media managers, and other DoD personnel operating official individual accounts must ensure all content is reviewed and approved for public release in accordance with DoDIs 5230.09 and 5230.29, as applicable.

d. While not exhaustive, the following restrictions apply to the official use of social media by DoD personnel. Restrictions pertaining to the personal use of social media by DoD personnel are addressed in Section 8 of this instruction and in the standards of conduct that apply to DoD personnel through DoD 5500.07-R and applicable Office of Government Ethics regulations.

(1) Misuse of Position.

DoD personnel will not:

(a) Use their official position or public office for private gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives, or other acquaintances.

(b) Use or permit the use of their government position or title or any authority associated with their public office in a manner that is intended to coerce or induce another person to provide any benefit, financial or otherwise, to themselves or to friends, relatives, or persons with whom the employees are affiliated in a nongovernmental capacity.

(c) Use their government position or title in a manner that could reasonably be construed to imply that the government endorses or sanctions their personal activities or those of another. The use of one's official position or public office may include the use of any reference to one's status, name, image, or likeness as a DoD employee or member of the uniformed services.

(2) Use of Government Time and Property.

Section 2635 of Title 5, Code of Federal Regulations and DoD 5500.07-R require that DoD personnel use official time in an honest effort to perform official duties. These regulations and standards also require employees and Service members to protect and conserve government

property and to use government property only to perform official duties, unless they are authorized to use government property for other purposes.

(3) Use of Non-Public Information.

(a) DoD personnel may not disclose non-public information on official or personal social media accounts. They will not allow the improper use of non-public information to further their own private interest or that of another.

(b) PA offices, social media managers, and other DoD personnel operating EOP accounts will report known or suspected occurrences of information on the accounts that is not authorized for release to their Component's security office and insider threat hub, and respond based on applicable DoD policy.

(4) Misuse of Personal Accounts.

DoD personnel must only use official DoD social media accounts to disseminate official information. DoD personnel are prohibited from using personal social media accounts for official purposes, including for conveying DoD information or official DoD positions. This does not prohibit using personal social media accounts to forward, like, or link to official information, provided it is done in a manner that does not express or imply DoD sanction or endorsement of any personal content.

(5) Political Activity.

(a) Engaging in political activity on official DoD social media and EOP platforms is prohibited. Additionally, DoD personnel may not engage in political activity, on their personal social media, while in the Federal workplace or while on-duty including while teleworking. Political activity is defined as an activity directed toward the success or failure of a political party, candidate for partisan political office or partisan political group.

(b) Certain DoD personnel have additional restrictions. Guidance on political activity restrictions is available from the DoD Standards of Conduct Office, <https://dodsoco.ogc.osd.mil/>.

(6) Discrimination, Harassment, and Extremism.

In accordance with DoDI 1020.03 and DoDI 1020.04, all DoD personnel must maintain an appropriate level of professional conduct and treat others in the workplace with dignity and respect. Military personnel are prohibited from actively participating in extremist activities in accordance with DoDI 1325.06, which can include activity on social media. At all times, DoD personnel must adhere to the terms of service and community guidelines dictated by the social media platform and to applicable DoD discrimination, harassment, and extremism policies. On official DoD social media and EOP platforms, engaging in activities that are illegal, inappropriate, or offensive to fellow users or to the public is prohibited. Such activities include, but are not limited to:

(a) Hate speech or material that ridicules others on the basis of race, religion, color, sex, disability, national origin, gender-identity, or sexual orientation.

(b) Speech or material promoting violent extremist or terrorist activities.

(c) Speech or materials advocating the overthrow of the government.

(7) Children.

Agency social media accounts may not collect any personal information from children (i.e., individuals under the age of 13), consistent with the standards of the Children's Online Privacy Protection Act (Section 6501-6506 of Title 15, U.S.C.) as applied to Federal agencies by Office of Management and Budget Memorandum M-03-22.

(8) Professionalism.

DoD personnel will at all times adhere to applicable standards of professionalism, including as provided in this issuance.

(9) Possible Collection of Personally Identifiable Information (PII).

All DoD personnel must limit the collection, use, maintenance, and dissemination of PII in accordance with DoDI 5400.11.

6.2. PA OFFICIAL USE OF SOCIAL MEDIA.

There are three types of official social media accounts for official use within DoD: organizational, institutional, and individual. These account types are used to release official DoD information and visual information materials. Any public disclosures must comply with DoDI 5230.09 and DoDI 5230.29, as applicable.

a. Official Organizational Accounts.

Official organizational accounts communicate on behalf of the DoD or OSD Component or program, and are representative of the DoD and Federal Government digital presence for public information (e.g., @USArmy or @DeptofDefense). Organizational accounts are communication platforms of an agency's digital brand strategy and managed by a team that has access to the account to publish content that supports a communication plan.

b. Official Institutional Accounts.

(1) Official institutional accounts are denominated only with an official position title (e.g., @SecDef, @DepSecDef) and are not associated with a personal name. These accounts are managed by the individual in the position in coordination with a PA office.

(2) When the official vacates the position, social media managers will archive the content of their account. PA representatives will assess the communication value to transition the account to the incoming official or archive the account. The out-going official is prohibited from maintaining the account. If the account is archived, PA and social media managers will

inform audiences that the account is no longer maintained and redirect users to platforms or accounts that will provide information of similar interest.

c. Official Individual Accounts.

(1) Official individual accounts include a personal name or identifier (e.g., @DASDSmith). Individual accounts are the least preferred account type due to the custom name associated with a position title.

(2) Individuals may not merge, rename, or convert a personal account or prior non-DoD account into a DoD EOP.

(3) Individuals serving in DoD who assume a new position and title within DoD may not merge, rename, or convert a prior official individual account to a personal account. The prior individual account expires once the individual is no longer associated with the position or title.

(4) Individuals with an official DoD individual account who depart DoD may not merge, rename, or convert the official DoD individual account into another account, personal or otherwise. The prior DoD individual account expires once the individual is no longer associated with the DoD position or title.

(5) Individuals from one OSD or DoD Component who are assigned to another joint, interagency, intergovernmental, or multinational entity may establish an EOP for their position in this new entity in accordance with Paragraph 4.1. The social media account is non-transferrable and expires once the individual is no longer associated with that entity.

6.3. MILITARY MARKETING AND RECRUITMENT ACCOUNTS.

Although this issuance does not apply to military recruitment/marketing accounts, social media accounts for PA activities may support local or national recruitment efforts by amplifying appropriate content on their account. In accordance with DoDI 1304.35, recruiting personnel will coordinate with local PA chiefs when conducting marketing engagement or other community events, in accordance with Paragraph 3.3 of DoDI 1304.35.

SECTION 7: MAINTAINING AN EOP

7.1. RECORDS MANAGEMENT.

a. DoD Information Security

DoD personnel must ensure that only information authorized for release is released to the public via social media, in accordance with DoDIs 5230.09 and 5230.29, as applicable.

b. Managing Social Media Records.

(1) Any content posted by DoD to an EOP is an official communication, regardless of the format.

(2) The records associated with the EOP will be managed in accordance with the appropriate OSD or DoD Component records schedule pursuant to Part 1226 of Title 36, Code of Federal Regulations.

(3) A complete social media Federal record must have content, context, and structure, along with associated metadata. The complete record must be maintained pursuant to OSD or DoD Component records management policies and procedures to ensure reliability and authenticity.

(4) Derogatory, inappropriate, and offensive content posted on an EOP by a user on the platform must be addressed in accordance with the terms of service and acceptable online conduct guidelines. Social media and records managers should evaluate the content in context, including whether a DoD response was provided, to determine if the post is a Federal record.

c. Capturing Social Media.

(1) Social media managers and other DoD personnel responsible for retaining social media content on behalf of their component can use the following non-exhaustive list of questions to help determine the appropriate disposition authorities applicable to a social media post:

(a) Does it contain evidence of the department or agency's policies, business, or mission?

(b) Is the information only available on the social media site?

(c) Does the agency use the social media platform to convey official agency information?

(d) Is there a business need for the information?

(2) Methods to capture social media records include:

- (a) Using web crawling or other software to create local versions of sites.
- (b) Using web capture tools to capture social media.
- (c) Using platform-specific application programming interfaces to pull content.
- (d) Using Really Simple Syndication feeds, aggregators, or manual methods to capture content.
- (e) Using tools built into some social media platforms to export content.

(3) The options for successful social media capture will depend on the technical configuration of a social media platform. Component needs may also affect which social media capture method is used. Once the Component determines the capture method, they must provide training to applicable staff on how and when to use capture tools for social media. Components may need to work with third-party providers to implement social media capture.

d. Private or Direct Messages from DoD Social Media Accounts.

- (1) Engaging in private or direct messaging to communicate official DoD information from DoD social media accounts should be conducted with care.
- (2) Private or direct messaging is allowed if PA and social media managers identify a specific need to remain responsive to authentic public interest or questions.
- (3) Due to potential preservation issues, DoD social media accounts may not send direct or private electronic messages that automatically expire.
- (4) If public comments on or to a DoD social media account warrant a non-public response, the DoD social media account manager(s) should publicly comment on the post(s) and suggest the individual(s) email the specific question(s) to the official DoD email account displayed in the profile.

e. Account Transition and Archiving of Official Social Media Accounts.

Consistent with Paragraph 6.2 of this instruction, DoD personnel operating an EOP may not retain official accounts or access to any official accounts in a personal capacity after departing the government or the government position associated with the account, as applicable.

(1) Official Organizational and Institutional Accounts.

(a) Within 30 days after the departure of the official associated with the institutional account, content posted to the account during the departing official's tenure must be managed and preserved in accordance with the proper records schedule.

(b) OSD and DoD Components should follow the most pertinent records schedule, in consultation with their records manager, because not every Component has a records schedule

specific to social media records. This is to ensure the records are preserved appropriately if the new official chooses not to use the previously established official presence.

(c) On the final day of activity for the account, PA and social media managers will post a final message, and provide the password and login information to the designated point of contact for use by the next official.

(d) If the new official indicates he or she does not want to use the official institutional account before the account holder's final day of service, the account should be closed, and the associated records managed in accordance with the proper records schedule.

(2) Official Individual Account.

Within 30 business days after the departure of the official associated with the official individual account, all content posted to the account during the departing official's tenure must be managed and preserved in accordance with the proper records schedule. On the final day of activity for the account, the account will issue its final content and the account will be closed.

7.2. USE OF PAI FOR PA.

a. Public engagement on social media platforms requires situational awareness of the information environment. PAI enables PA to generate audience insights, provides social media trend analysis, and inform leaders of emerging communication crises. In accordance with DoDD 3115.18, and Appendix 3A of DoDI 8170.01, PA offices may access and use PAI for PA activities.

b. PA offices may use third-party social media management platforms or services to manage official social media accounts. OSD and DoD Component PA offices must follow acquisition processes and procedures to obtain authorization for software or services. PA offices may need to coordinate with relevant Component offices, including their Chief Information Officer, for additional instructions, guidance, and policy to access third-party or commercial off-the-shelf services to access PAI.

c. PA offices with authorization and authority to use third-party social media management platforms must maintain records management procedures in accordance with Paragraph 7.1.

d. PA offices will coordinate with their local records manager for specific guidance and recommendations to capture and schedule records through third-party content scheduling platforms, if the platform or service has the capability or function to capture social media records. PA offices default to capturing and scheduling records directly from the social media platform if the content scheduling platform is inadequate or incapable of providing content, context, and structure along with associated metadata for records management.

7.3. RISKS ASSOCIATED WITH OPERATING EOP.

a. Social Media Cyber-Vandalism.

(1) Responding to cyber-vandalism events involving official social media accounts is the responsibility of multiple officials including, but not limited to, PA officials, social media account manager(s), legal advisors, and information technology security personnel. These key personnel form the response team that must establish incident response procedures, consistent with DoDIs 8500.01 and 8170.01. The response team must exercise and rehearse various scenarios to quickly assess, recover, and respond to an incident. The response team manages the process to ensure all elements of the incident are reported and addressed. The response team will determine when the incident is closed.

(2) The response team should conduct an incident after-action report and assessment to review, update, or draft procedural tasks, regulations, or policy.

(3) A template response to cyber-vandalism is provided through the General Services Administration's Technology Transformation Services at <https://digital.gov/resources/readiness-recovery-response-social-media-cyber-vandalism-toolkit/>. The response team should amend and adapt the template as necessary to conform to its Component's guidance, regulations, and policies.

b. Fake or Imposter Social Media Accounts of DoD Employees and Service Members.

Users, malign actors, and adversaries on social media platforms may attempt to impersonate DoD employees and Service members to disrupt online activity, distract audiences from official accounts, discredit DoD information, or manipulate audiences through disinformation campaigns. PA offices managing an EOP must address fake or imposter accounts.

(1) Reporting Fake or Imposter Social Media Accounts.

(a) PA chiefs and social media managers must report fake or imposter accounts through the social media platform's reporting system. Social media platforms and applications establish the information requirements to report such accounts. PA offices must establish local procedures to identify, review, and report fake or imposter accounts. PA and social media managers must notify operations security officials of fake or imposter accounts, as well as cyber operations, counterintelligence elements, and Military Department Counterintelligence Organization in accordance with DoDD 5240.06

(b) PA chiefs and social media managers must record the reporting of fake or imposter accounts.

(c) PA chiefs or social media managers may need to provide additional information as evidence that the identified account is fake or impersonating a DoD official.

(2) Indications or Common Identifiers Associated with Imposter Accounts.

Indications or common identifiers associated with imposter accounts include, but are not limited to the following:

- (a) The account is not registered as an official DoD account.
- (b) The account has very few photos that were recently uploaded and reflect the same date range.
- (c) The account has very few followers and comments.
- (d) The account sends friend requests to individual users on the platform.
- (e) The account name and photos do not match.
- (f) There are obvious grammatical or spelling errors.
- (g) Key information is missing.

7.4. LINKING AND SHARING FROM OFFICIAL SOCIAL MEDIA ACCOUNTS.

a. In accordance with DoDI 8170.01, OSD and DoD Components may establish hyperlinks only to information or services related to the performance of the DoD Component's function or mission and the purpose of the electronic messaging service. Any links from an official social media account must comply with DoDI 8170.01, section 3.20.

b. DoD cannot endorse, sponsor or advertise on behalf of another non-government service, facility, event, or product. The use of external links on official accounts may convey a misrepresentation of government endorsement or provide an incorrect interpretation of DoD policy, position, or message. DoD officials, PA chiefs, and social media managers of EOP must assess the information value of the source before sharing an external link by considering factors including, but not limited to, the author and publisher's credibility, the validity of the information at the source, the references or subject matter experts cited within the source, and whether the information is true and factual. When external links to non-U.S. Government websites are posted on official social media accounts, content managers will include the following disclaimer: "The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense of the linked websites, or the information, products or services contained therein. Other than for authorized activities, such as military exchanges and Morale, Welfare and Recreation sites, the United States Department of Defense does not exercise any editorial control over the information you may find at these locations." Content managers will not direct users to paid sites or subscription services.

c. OSD and DoD Component EOPs may link and share content found on DoD-registered, public-facing websites, and social media platforms without formal coordination.

d. PA and social media managers will establish local guidelines to share external links from non-DoD sources that support PA activities, including a specific, mission-essential reason or a Commander's information objective(s) in accordance with DoDI 8170.01.

7.5. SOCIAL MEDIA PLATFORM VERIFIED ACCOUNTS.

a. EOPs registered with DoD do not need to display a "verified" status with the social media platform to be recognized by DoD as an official account. While PA chiefs and social media managers should attempt to have an EOP recognized as a verified account by the social media platform for all account types, they are not required to do so. All registered EOPs in the DoD registry or the U.S. Digital Registry are official accounts, in accordance with Paragraph 4.1.b.

b. A "verified" personal account on a social media platform does not constitute an official DoD account. Personal accounts that are "verified" as a government account by a social media platform may be misconstrued as an official DoD account.

SECTION 8: PERSONAL SOCIAL MEDIA USE BY DoD PERSONNEL

DoD personnel may use unofficial personal social media. In doing so, DoD personnel must adhere to the rules discussed in this instruction, including preventing the unauthorized disclosure of non-public information (or unclassified information that aggregates to reveal classified information) and refraining from any appearance of DoD endorsement or sanction. The following guidance applies to DoD personnel who maintain a personal social media presence.

a. Maintain a Clear Distinction Between Personal and Official Accounts.

(1) DoD personnel must ensure that all personal social media accounts are clearly identifiable as personal accounts. DoD personnel must ensure that their personal social media accounts avoid use of DoD titles, insignia, uniforms, or symbols in a way that could imply DoD sanction or endorsement of the content. DoD personnel should use personal, non-official contact information, such as personal telephone numbers or postal and e-mail addresses, to establish personal, nonofficial accounts.

(2) Where confusion or doubt is likely to arise regarding the personal nature of social media activities, personnel are encouraged to include a disclaimer clarifying that their social media communications reflect only their personal views and do not necessarily represent the views of their agency or the United States. (See sample disclaimer Figure 2.) The use of a disclaimer does not otherwise allow DoD personnel to accept compensation that is prohibited by this instruction or other applicable regulations.

Figure 2 Sample Disclaimer for Personal Social Media Accounts

The views and opinions presented herein are those of the author and do not necessarily represent the views of DoD or its Components. Appearance of, or reference to, any commercial products or services does not constitute DoD endorsement of those products or services. The appearance of external hyperlinks does not constitute DoD endorsement of the linked websites, or the information, products or services therein.

(3) DoD personnel are not prohibited from using personal social media accounts to forward, like, or link to official information, provided it is done in a manner that does not express or imply DoD sanction or endorsement of any personal content.

b. Do Not Disclose Non-Public Information.

DoD personnel are prohibited from disclosing non-public information to further their private interests or the private interests of others. Additionally, DoD personnel must adhere to operations security and unit-level directives, including while in forward-operating environments. Release of unauthorized content through any means, including social media, may unnecessarily hazard individuals, units, and the mission.

c. Do Not Conduct Official Business on Personal Social Media Accounts.

(1) Personal accounts may not be used to conduct official DoD communications, in accordance with Paragraph 3.26.a of DoDI 8170.01 and Section 2911 of Title 44, U.S.C.

(2) A personal social media account must not be an avenue for friends, followers, or private contacts to gain access to DoD programs or seek action from DoD officials in a manner not available to the general public.

d. Do Not Accept Compensation for any Activity Relating to One's Status as a DoD Civilian Employee or Military Service Member.

DoD personnel are prohibited from using their official position or public office for personal financial gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives, or persons with whom the employee is affiliated in a nongovernmental capacity. (Section 2635.702 of Title 5, CFR). DoD personnel are also prohibited from using government resources for non-official, personal activities.

(1) Use of Official Position or Public Office.

The use of one's official position or public office includes the use of any reference to one's status, name, image, or likeness as a DoD civilian employee or Service member. This includes the use of official titles, photographs that display a connection to one's status as a DoD civilian employee or Service member (e.g., a photograph while in uniform or while wearing an identifying device such as a lanyard or lapel pin); and the personal use of DoD protected symbols or other imagery.

(2) Endorsement.

DoD personnel are prohibited from using their official position to either affirmatively endorse a non-federal entity, product, service, or enterprise, or by taking action that implies DoD endorsement through the unauthorized use of one's official position or public office.

(3) Private Gain.

Private gain includes the receipt of compensation from a third party, to include revenue from advertising, sponsorships or sponsorship agreements, affiliate marketing agreements, or promotion of commercial ventures on personal social media accounts. This does not preclude DoD personnel from engaging in compensated outside employment when permitted by applicable ethics and other regulations.

e. Do Not Engage in Prohibited Political Activity, as Defined in Applicable Law and Regulation.

See Paragraph 6.1.d.(5) of this instruction.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ATSD(PA)	Assistant to the Secretary of Defense for Public Affairs
DoDD	DoD directive
DoDI	DoD instruction
EOP	external official presence
PA	public affairs
PAI	publicly available information
U.S.C.	United States Code

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
counterintelligence	Defined in DoDD 5240.02.
DoD personnel	DoD civilian employees and military service members. For purposes of this issuance, “DoD personnel” does not include employees of DoD contractors.
electronic messaging services	Defined in DoDI 8170.01.
EOP	Defined in DoDI 8170.01.
Federal record	A “record” as defined in Section 3301 of Title 44, U.S.C.
manager	DoD employee or Service member responsible for managing DoD social media EOPs.
marketing	Defined in DoDI 1304.35.
Military Department Counterintelligence Organization	Defined in DoDD 5240.02.

TERM	DEFINITION
non-public information	Defined in DoD 5500.07-R.
PAI	Defined in DoDD 3115.18.
personal account	Non-DoD-controlled electronic messaging services account intended for personal use and not associated with official DoD functions.
social media platform	Non-DoD-controlled electronic messaging service with publicly accessible information capabilities and applications available across the internet that facilitates the sharing of user-generated content through virtual connections, networks, and communities through a computer or mobile device.
social media cyber-vandalism	An intrusion of social media accounts when an outside party takes control of an agency communication channel, establishes an impostor DoD social media account, or impersonates a DoD official using a social media account in an attempt to mislead the public or threaten the agency or the individual account.
terms of service	Defined in DoDI 8170.01.
third-party social media management platforms	Free or paid social media management tools that can schedule content and generate social media reports to improve audience engagement and manage social media platform capabilities.
verified account	A moniker or symbol which notifies users on the social media platform that the account of public interest is authentic and helps reassure users to trust the information on the account.

REFERENCES

- Code of Federal Regulations, Title 5, Section 2635
- Code of Federal Regulations, Title 36, Part 1226
- DoD 5500.07-R, “Joint Ethics Regulation (JER),” August 30 1993, as amended
- DoD Directive 3115.18, “DoD Access to and Use of Publicly Available Information (PAI),” June 11, 2019, as amended
- DoD Directive 5122.05, “Assistant to The Secretary of Defense for Public Affairs (ATSD(PA)),” August 7, 2017
- DoD Directive 5240.02, “Counterintelligence (CI),” March 17, 2015, as amended
- DoD Directive 5240.06, “Counterintelligence Awareness and Reporting (CIAR),” May 17, 2011, as amended
- DoD Directive 5535.09, “DoD Branding and Trademark Licensing Program,” December 19, 2007
- DoD Instruction 1020.03, “Harassment Prevention and Response in the Armed Forces,” February 8, 2018, as amended
- DoD Instruction 1020.04, “Harassment Prevention and Responses for DoD Civilian Employees,” June 30, 2020
- DoD Instruction 1304.35, “Military Marketing,” November 1, 2017, as amended
- DoD Instruction 1325.06, “Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces,” November 27, 2009, as amended
- DoD Instruction 5015.02, “DoD Records Management Program,” February 24, 2015, as amended
- DoD Instruction 5230.09, “Clearance of DoD Information for Public Release,” January 25, 2019, as amended
- DoD Instruction 5230.29, “Security and Policy Review of DoD Information for Public Release,” August 13, 2014, as amended
- DoD Instruction 5400.11, “DoD Privacy and Civil Liberties Programs,” January 29, 2019, as amended
- DoD Instruction 5400.13, “Public Affairs (PA) Operations,” October 15, 2008
- DoD Instruction 8170.01, “Online Information Management and Electronic Messaging,” January 2, 2019, as amended
- DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014, as amended
- Office of Government Ethics’ (OGE) Legal Advisory, LA-14-08, “Reference to Official Title and Position by Employees Affiliated with Outside Organizations in Their Personal Capacity,” November 19, 2014
- Office of Government Ethics’ (OGE) Legal Advisory, LA-15-03, “The Standards of Conduct as Applied to Personal Social Media Use,” April 9, 2015
- Office of Management and Budget Memorandum M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” September 26, 2003
- United States Code, Title 5
- United States Code, Title 15
- United States Code, Title 44
- REFERENCES

Page Intentionally Left Blank

For social media queries
please email:
NavySM@us.navy.mil